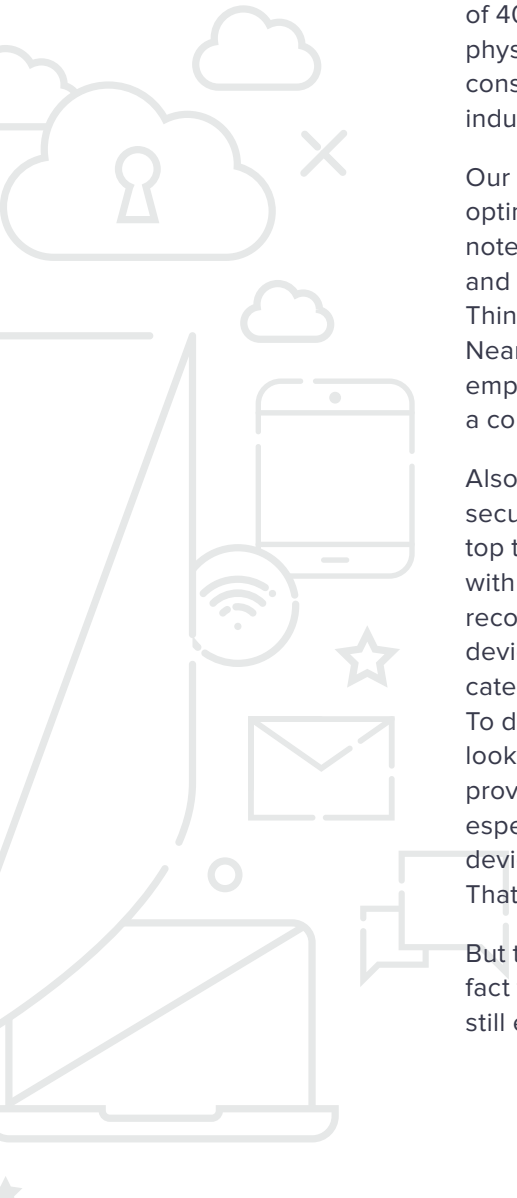
White Paper

A Study of IoT-Connected Product Security: Best Practices and Common Pitfalls to Avoid

By Paul Roberts, Editor in Chief, The Security Ledger

xively™ by LogMeIn

Rather than bolting security on to finished products, device makers need to build it in from the earliest stages of product development...



IN AN EFFORT TO BETTER THE SECURITY strategy and plans of connected device makers, The Security Ledger and LogMeIn have collaborated on a survey of 400 professionals at firms making physical products in industries including consumer electronics, “smart” home, industry and life sciences.

Our study found reasons for both optimism and concern. On a positive note, there is strong interest in designing and adapting products for the Internet of Things (IoT)among survey respondents. Nearly three-quarters said that their employer has—or is working on—a connected product.

Also encouraging is the finding that security and stability are far and away the top two concerns among device makers, with companies from various industries recognizing the need to better secure devices from malicious software, sophisticated hackers and other online attacks. To do so, the companies we surveyed are looking to trusted partners and service providers to shoulder some of the load, especially in areas like user identity and device provisioning and management. That’s good news.

But there are warning signs, including the fact that significant gaps in understanding still exist within this population of device makers. That is especially true in areas such as risk assessment and mitigation.

Survey respondents showed a keen awareness of the risks posed by sophisticated and remote hackers and the dangers of data leaks from connected devices. However, other well-established risks such as account hijacking, software supply chain risks and denial of service attacks registered more faintly with them. If device makers fail to adequately address the most common risks to connected devices, the result may be a population of deployed devices with less robust security features that open the door to future generations of hackers.

We believe that more education is needed to increase awareness of unique IoT security risks within the developer community so that development resources are directed where they will make the biggest difference. Also, rather than bolting security on to finished products, device makers need to build it in from the earliest stages of product development and, where possible, tap reliable partners with experience securing and managing connected devices at scale.

Index

Introduction

IoT is ushering in whole new categories of products and services, but it is also creating novel opportunities for cybercriminals and other malicious actors to infiltrate networks and gain unauthorized access to data and systems.

KEY TAKEAWAYS

- There will be billions of connected, smart devices by the end of the decade.
- Much of the burden will fall to device makers to create secure and robust products that model best practices in software security design.
- Vulnerabilities in a single, popular piece of code can affect hundreds, thousands or even millions of deployed devices.

WHEN TECHNOLOGY INDUSTRY professionals talk about the growth of the Internet of Things, what they most often talk about are the big numbers—the billions. That refers to the oft-voiced prediction that there will be billions of connected, smart devices by the end of the decade. How many billions is a matter of debate. Estimates range from 50 billion (Cisco) to a more modest 20.4 billion (Gartner) or even fewer.

Regardless of what the number turns out to be, it will be big. (Gartner, for example, estimates that as many as 8.5 billion devices are already connected to the Internet of Things). But whose devices are they and who—or what—is responsible for administering them? That's a tricky question. As it stands, the responsibility for managing those billions of devices sits with a loosely joined group of players: the device owners, the manufacturers and their third-party suppliers, and infrastructure owners like telecommunications companies. Absent any central authority to enforce IoT security, much of the burden will fall to device makers to create secure and robust products that model best practices in software security design.

Will those firms rise to the challenge? So far, the signs are not encouraging. The emergence of the Mirai, Persirai and Brickerbot botnets suggest that connected devices are being deployed in homes and businesses with only cursory protections or with no protections at all.

> ...cybercriminals often have no need to exploit hidden software vulnerabilities. Instead, they take advantage of default usernames and passwords that are widely shared to gain access to administrative features on connected cameras, digital video recorders and other endpoints.

News accounts may describe these botnets as consisting of "hacked" devices. But the sad truth is that cybercriminals often have no need to exploit hidden software vulnerabilities. Instead, they take advantage of default usernames and passwords that are widely shared to gain access to administrative features on connected cameras, digital video recorders and other endpoints. Inconsequential by themselves, these devices are devastating in aggregate as they can be assembled into massive networks that carry out denial of service attacks against unsuspecting web sites and Internet infrastructure.

The world has also learned that the use and reuse of shared components, from open source and proprietary operating systems and software libraries to low-cost hardware, poses a huge and still-underappreciated risk. Vulnerabilities in a single, popular piece of code can affect hundreds, thousands or even millions of deployed devices, as we've seen with the Heartbleed vulnerability in Secure Sockets Layer or the "Devil's Ivy" vulnerability in the gSOAP open source library.[1]

Security professionals will tell you that building security into products from the beginning is the best way to stem attacks and compromises. Firms like Microsoft, which is no stranger to the attentions of sophisticated hackers, have long advocated approaches like the SD3+C framework: Secure by Design, Secure by Default, Secure in Deployment and Communications.

But what about the individuals tasked with creating new, smart connected products? What kinds of products are they developing and for whom? What are their priorities and concerns as executives, product managers or developers?

1. http://blog.senr.io/blog/devils-ivy-flaw-in-widely-used-third-party-code-impacts-millions

About the Survey

By speaking directly to device makers, we sought to understand the security priorities of the organizations that will be producing the next generation of connected products.

KEY TAKEAWAYS

- Internet connectivity and interactivity are priorities for companies across industries.
- In short order, almost all products will be smart products.
- Going forward, challenges like device management and support loom larger than "advanced persistent threat" hackers.
- The companies reflected in our survey results ranged from large enterprises to small businesses.

OUR SURVEY OF 400 EXECUTIVES, product architects, designers and product managers found that the Internet of Things looms large across all industries. Internet connectivity and interactivity are priorities for companies across industries—whether they're managing existing products or attempting to launch their first. Technology industry boosters tell us that, in short order, almost all products will be smart products. Our survey supports that conclusion, though IoT deployments may fall short of the "millions" and "billions" of devices we hear about in breathless news reports.

But will those deployments be secure? On that question, our poll found that would-be connected device makers may be missing the forest for the trees: focusing on threats posed by skilled and determined hackers while giving a lower priority to what have already emerged as common sources of Internet of Things risk.

Going forward, challenges like device management and support loom larger than "advanced persistent threat" hackers. Weak authentication and identity schemas as well as risks posed by software and hardware supply chain partners threaten to undermine the best efforts of product designers and developers. That makes the need for trusted third-party partners and platform providers even more acute as manufacturers and product designers navigate the tricky waters of IoT identity management, data protection and application security in a way that produces secure, robust and resilient connected products. Let's explore the survey results!

WHO WE TALKED TO

To better understand the thinking and plans of connected device makers, Security Ledger and LogMeIn surveyed 400 professionals at North American firms. Respondents were spread across a number of industries, with the biggest share of responses to our survey from employees at firms in the consumer electronics industry (22%). Employees at life sciences firms were the next biggest group (17%), followed by light industry (15%). Employees at smart home product firms—a focus of much IoT innovation—accounted for 13% of respondents. Other industries reflected in our survey were extractive industries like oil and coal (11%), power generation and distribution (8%) and alternative energy (7%).

The companies reflected in our survey results ranged from large enterprises to small businesses. The majority of respondents (51%) worked for companies with between 100 and 1,000 employees, while

Weak authentication and identity schemas as well as risks posed by software and hardware supply chain partners threaten to undermine the best efforts of product designers and developers.

nearly a quarter (23%) were employed by firms with between 1,000 and 5,000 employees. Around 16% worked for smaller firms with 100 or fewer employees, and a little more than 10% worked for large firms with more than 5,000 employees.

By and large, our respondents were senior-level employees or members of technical teams. Almost one in four (24%) were executives, including chief executive officers, chief information officers or chief technology officers. Vice presidents of product management or information technology were around 8% of respondents. Product and project managers combined made up nearly a quarter of respondents (23%). Software engineers and engineering managers combined to make up around 19% of respondents, while software application developers were around 7% of those who responded to the survey.

Full Steam Ahead to the Internet of Things

What did our survey reveal?

Here are some of the top-level trends that emerged from our survey data.

KEY TAKEAWAYS

- More than half (51%) said they worked for companies that were "currently developing one or more connected products" but had not yet deployed a connected product.
- Our survey suggests that device makers are planning for more modest deployments—at least in the near term.

READY (AND SECURE) OR NOT, the Internet of Things is coming. That's one unmistakable conclusion from our survey, which found a strong majority of respondents working for companies that were pursuing connected products.

More than half (51%) said they worked for companies that were "currently developing one or more connected products" but had not yet deployed a connected product. Add to that the 23% who identified themselves as working for companies that had "already developed and deployed one or more connected products," and you have close to three of four respondents working at firms that were actively developing or already supporting a connected or smart product. Just over a quarter (26%) said their company was still in the beginning stages: researching the development of its first connected product or looking to connect existing product(s) to the Internet.

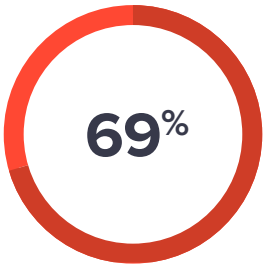
BILLIONS OF DEVICES? TRY THOUSANDS

While the popular press likes to play up the enormous size of the emerging Internet of Things, our survey suggests that device makers are planning for more modest deployments—at least in the near term.

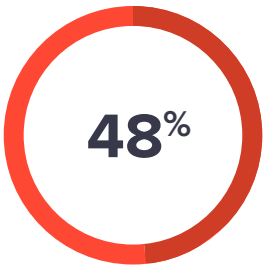
Asked how many devices their company anticipates having to support in five years,

a little more than a third of the respondents (37%) said the number would be in the tens of thousands of devices, while more than a quarter (26%) said the number of supported devices would measure in the thousands. Only 20% said they anticipated supporting hundreds of thousands of connected devices. Just 5% of those surveyed expected to be managing millions of devices five years from now.

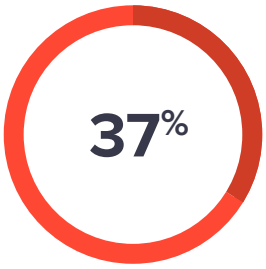
Consumer electronics leads the way. Whether a company was researching, developing or actively supporting a connected product had a lot to do with what kind of product it made, our survey found.



OF LIFE SCIENCES COMPANIES ARE DEVELOPING CONNECTED PRODUCTS



OF SMART HOME PRODUCT COMPANIES ARE DEVELOPING CONNECTED PRODUCTS



OF ELECTRONICS FIRMS ARE DEVELOPING CONNECTED PRODUCTS

FOR EXAMPLE, 30% of employees of firms that made consumer electronics and 27% of employees of smart home or business products said their employer has already deployed one or more connected products. Consumer electronics firms were also the most likely (33%) to be researching new connected products. That's more than double the figure for employees of life sciences companies, where just 13% said their company already had a smart product on the market.

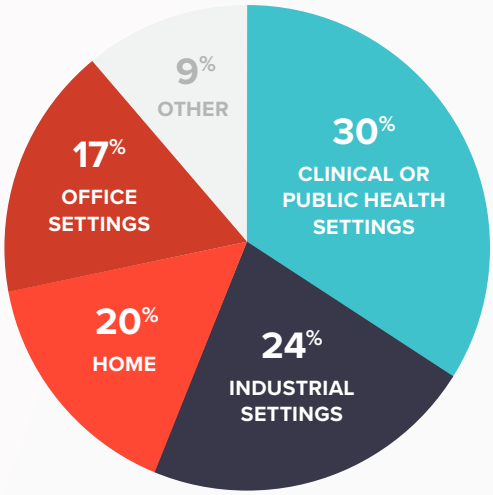
Flip it around, and survey respondents who worked in life sciences were much more likely to say that their employer was developing a connected product (69%) than were employees of consumer electronics firms (37%) or smart home product companies (48%). In other words: consumer firms were first to market with connected products, but a wide range of industries is close on their heels. We should expect a steady stream of smart products in industries like personal health and wellness in the months and years ahead.

And while the size of the firm in question doesn't seem to strongly correlate with whether a company was researching or developing a connected product, larger firms with more than 5,000 employees were almost twice as likely (42%) to have developed and deployed a connected product than were small firms with fewer than 100 employees (25%) or medium-size firms with between 100 and 5,000 employees (20%).

MANY REASONS TO CONNECT

Why connect your product? For the same reason that drives much product development: competition. More than a third of respondents (35%) cited pressure to differentiate from competitors (18%) or keep up with them (17%) as a reason to build a connected product or to add connectivity to an existing product. For many respondents (29%), connecting their product was about improving it. Smaller but meaningful shares of respondents cited the desire to realize new revenue opportunities (17%) or discover revenue opportunities in data collected by smart products (13%).

Survey respondents are working on connected devices for the following sectors:



AND WHILE THE PRESS AND PUBLIC might worry about the privacy implications of data-hungry connected products like smartphones, fitness trackers and home assistants, our respondents across industries shared similar aspirations for the data collected by their company's smart products. In about equal measure, they saw applications for developing profiles of customers, making real-time decisions and anticipating problems with deployed devices (aka "predictive maintenance").

Sharing insights with business partners or using collected data to tailor their products to the needs of their customers were also among the top reasons cited for building a connected product.

HEALTHCARE, INDUSTRY AND HOME ARE DESTINATIONS

Where will these connected products be deployed? While the popular image of the Internet of Things device may be of an Internet-connected home surveillance camera or a smart refrigerator, slightly less than a third of our respondents (30%) said that the device their company was working on would be used in clinical or public health settings. Another 24% said the product they were developing was intended for use in industrial settings, while 20% said it was intended for use in the home. Seventeen percent said the connected device their company was working on was intended for use in an office setting.

Product Security, Stability Are Top Priorities

In spite of headlines about vulnerable and compromised Internet of Things devices—or maybe because of them—the men and women who responded to our survey said that security and stability were their top priorities in designing a connected product—an encouraging sign.

KEY TAKEAWAYS

- Close to half of respondents who worked for companies that had already developed and deployed a connected product ranked security as a top priority.
- Perception of risk may be complicating the job of aligning device security with the actual risks.
- Encrypting communications to and from devices is a critical step to securing IoT deployments.
- IoT-platform-as-a-service and third-party providers are critical to helping companies accelerate development without sacrificing the security of the finished IoT product.

ASKED TO RANK THEIR PRIORITIES for their connected product on a scale of 1 (most important) to 7 (least important), our respondents told us that having a product that was the most stable and best performing in its class on the market was their top concern, with an average rank of 3.57 out of 7, followed closely by the desire to have the "most secure product of its class," which had an average rank of 3.62 out of 7.

It's encouraging that security-related responses far outranked priorities like getting a "minimally viable" product to market (avg. 4.94), sporting the most "fully featured" product (avg. 4.07) or having the richest data collection (avg. 4.07). This suggests that our worst fears about smart device makers may not be true, and that the stereotype of device makers that prioritize time to market and functionality over security doesn't apply—at least to the companies that participated in our survey.

Should we conclude that concerns about security are hitting home with device makers and would-be device makers? That may be the case, especially those with some experience in the market. Our survey found that employees of companies that already had one or more connected products on the market ranked security a notably higher priority (avg. 3.32) than did employees of companies that were still in the early stages of researching a connected product (avg. 3.84). In fact, close to half (43%) of respondents who worked for companies that had already developed and deployed a connected product ranked security as a top priority (1 or 2 out of 7). Just 30% of employees who worked for companies that were still researching or developing connected products ranked it that high.

...security-related responses far outranked priorities like getting a "minimally viable" product to market (avg. 4.94), sporting the most "fully featured" product (avg. 4.07) or having the richest data collection (avg. 4.07).

The focus on security carried across industries as well, though it is worth noting that respondents from life sciences firms ranked security far lower, on average, than respondents did overall (4.31 vs. 3.65 on a priority scale of 1-6). In fact, life sciences firms ranked functionality and data collection as higher priorities than security—a worrying and somewhat

confusing data point, given the intense media and regulatory attention to problems such as medical device security. As a point of contrast, respondents who worked for consumer electronics firms ranked security as a higher priority than those in other industries or respondents on average (3.38 vs. 3.65).

DRILLING DOWN: FOCUS ON MALICIOUS ATTACKS, SECURING DATA

Of course "security" is a monolithic term that encompasses a number of important but distinct areas. We wanted to elicit in finer detail the security priorities of our device makers as well as their understanding of the threats facing devices once they were deployed.

To that end, we asked respondents a series of questions designed to pinpoint their security priorities. What we found was that protecting against malicious attacks on devices was far and away the top security concern and priority. It scored an average ranking of 3.1 on a scale of 1 (most important) to 6 (least important) among those we surveyed. Protecting personally identifiable information (PII) was the next-highest-ranked priority, with a mean ranking of 3.39.

> ...respondents who worked for firms that already had a connected product deployed ranked protections against malicious attacks higher (2.96) than respondents did on average, and notably higher than respondents from companies that were still researching a connected product (3.17).

The concern about malicious attacks against deployed devices was also evident when we asked our survey takers to rank "cyber adversaries"—the threats they were most concerned about. There, also, skilled hackers (avg. 2.93 on scale of 1–8) and cybercriminal groups (avg. 2.96) rated as the biggest concerns for our respondents, topping out endemic problems like weak communications security and authentication. (We'll talk later about why this might be a problem.)

There, respondents who worked for firms that already had a connected product deployed ranked protections against malicious attacks higher (2.96) than respondents did on average, and notably higher than respondents from companies that were still researching a connected product (3.17).

BEWARE OF "MR. ROBOT"

Looked at objectively, the concern about malicious hacks carried out by sophisticated attackers is understandable. Data theft is one of the most widely reported and recognized cyber threats. The headlines have been filled with stories about high-profile hacks of leading retailers like TJX,

So it should not be surprising then that high-skill hackers rate as a top concern for our respondents, while threats from low-skill hackers—"script kiddies"—were considered a lower risk than "ordinary users"...

KEY POINT

Remote, software-based attacks on devices were the biggest concern for survey respondents.

Best Buy and Home Depot for much of the past decade. More recently, hospital networks, health insurers and electronic health records firms have been the targets.

While data theft isn't typically the motivation for attacks on connected devices—at least not so far—it's understandable that device makers would be concerned about the risk of data theft to devices they deploy.

Similarly, popular media accounts of hacks of connected devices—ranging from reports in the mainstream media to popular shows like "Mr. Robot"—hold out the specter of threats to connected stuff from sophisticated actors and cybercriminal groups. Even among informed industry professionals, reports about device vulnerabilities typically come from talented and skilled security researchers who are able to delve into and expose the workings of connected products and discover software or design flaws.

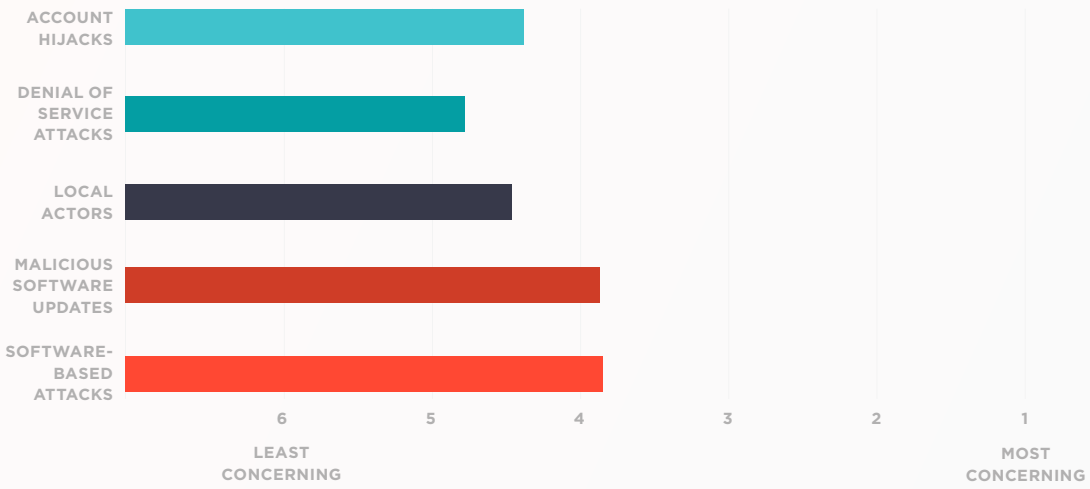
So it should not be surprising, then, that high-skill hackers rate as a top concern for our respondents, while threats from low-skill hackers—"script kiddies"—were considered a lower risk than "ordinary users" (avg. 4.1 vs. 3.96 on a scale of 1-6).

"If anyone is going to hack our product," our respondents seem to be saying, "they'd better be good!"

Similarly, incidents like the Mirai botnet attack that took out managed domain name system provider DYN have been depicted as a sophisticated operations with considerable downstream consequences, including the disruption of service for major Internet providers and sites like Amazon.com and Spotify. It makes sense, then, that device makers would see such threats as their biggest concern. Nobody wants their devices to be the backbone for the next Mirai.

THE THREAT 'OUT THERE'

Our respondents are convinced that attacks on devices—when they come—will come from the outside. Asked to rank threats to connected devices, the men and women who responded to our poll said that remote, software-based attacks on devices were their biggest concern (3.92 on a severity scale of 1-6), just ahead of malicious software updates (3.93) Those threats notably out-polled threats from local actors (4.4) as well as other common attacks like account hijacks (4.38) and even denial of service attacks (4.72).



Respondent's top security concerns are focused on sophisticated, malicious attacks, such a DDOS.

The picture that emerges from our deep dive on cyber adversaries is of a device maker population that is concerned about attacks from sophisticated actors on the outside with the skill and determination to hack into connected devices. Those are valid concerns, to be sure, especially in an environment in which threats like ransomware and nation-state hacking are on the rise. But should they be the top concerns for device makers? That's what we'll discuss next.

ON SECURITY: MISSING THE FOREST FOR THE TREES?

As we've noted, the good news from our survey is that device makers take the security of their connected products seriously—ranking it as their second-highest priority behind stability and performance.

The bad news may be that those same employees are focused on the wrong set of security threats and problems, or at least a set of problems that are less urgent and that will be difficult for device makers to address in a meaningful way. In the process, device makers, at least those represented by our survey population, may be overlooking a host of problems and threats that they are in a position to address, and that would make a meaningful impact on the security and integrity of deployed devices.

KEY POINT

Both experts and recent events show us that DDoS attacks are common and popular, as they don't require intimate knowledge of the device being targeted or any skill to carry out.

Take a problem like account hijacking as one example. This type of attack, in which a cyber adversary takes over the account of a legitimate user, is among the most common types of attacks on connected devices. Account takeover attacks were, for example, the primary means by which the Mirai botnet was built. The Mirai malware was programmed to scan the network to which it was connected for devices, guessing at usernames and passwords to access those devices using a list of default administrator credentials. When a matching user and password combination was found, the attackers used their access to the device to upload the Mirai software and move on to the next target.

Many other attacks on Internet of Things devices have and continue to use the same approach: making use of documented, default credentials or taking advantage of configuration weaknesses (like the absence of a "time out" feature to curtail failed login attempts) to get control of a device.

Despite that, account hijacking attacks were rated a lower risk (4.38 on a severity scale of 1 to 8) than more obscure attacks like malicious software updates (avg. 3.93 on the same severity scale) or unwanted attention from a security researcher (avg. 3.67) or low-skill hacker (avg. 4.11).

Similarly, distributed denial of service attacks (DDoS) ranked low (avg. 4.72) when put side to side with threats like remote software attacks or operations by cybercriminal gangs, even though both experts and recent events show us that DDoS attacks are common and popular, as they don't require intimate knowledge of the device being targeted or any skill to carry out.

Our respondents considered endemic security problems like weak transport (or communications) security (4.82), device impersonation ("spoofing") (4.63) and vulnerable mobile applications (5.04) relatively low priorities, even though documented incidents of attacks against connected devices have illustrated that attackers frequently target just such vulnerabilities in connected devices.

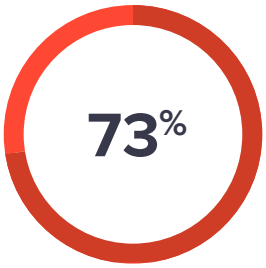
What's going on? One explanation is that our respondents' concerns about securing their devices are a product of their perception (and the popular perception) of cyber threats as coming from external actors—faceless hackers and cybercriminals "out there" beyond the firewall.

Our respondents considered endemic security problems like weak transport (or communications) security (4.82), device impersonation ("spoofing") (4.63) and vulnerable mobile applications (5.04) relatively low priorities, even though documented incidents of attacks against connected devices have illustrated that attackers frequently target just such vulnerabilities in connected devices.

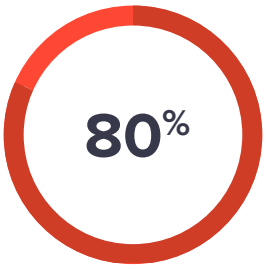
It is certainly not wrong for device makers and would-be device makers to worry about such problems. But their perception of risk may be complicating the job of aligning device security with the actual risks to the specific device and the known history of attacks against similar devices. Most attacks are not novel but take advantage of inherent and often-documented weaknesses in how products are designed, coded or deployed. More accurate risk assessments would, for example, presumably elevate the importance of exposures like account hijacking, device impersonation, insecure mobile applications and DDoS attacks over the greater threat posed by external actors. Our survey suggests that, absent such a risk-based approach, much of the low-hanging fruit of connected device security will remain unpicked. For example, less than half (45%) of respondents said they would secure connected device deployments by using encrypting communications to and from their deployed devices using technologies like TLS (transport layer security). Encrypting communications to and from devices is a critical step to securing IoT deployments, as unencrypted communications can expose user credentials as well as sensitive data. Still, only the smart home/smart business industry had a majority (52%) of respondents say that encrypted communications would be a feature of their connected products. In consumer electronics, the share was less than 40%.

Another unappreciated feature was mandatory updates to default administrator credentials. The Mirai botnet illustrated how default credentials, left unchanged, can open the door to hackers and online mayhem. Still, just 39% of our survey respondents indicated that their company's product would force customers to change the default administrator credentials. The numbers were a bit more encouraging among smart home and smart business product firms, where close to 47% said they would support that feature. Steps like restricting access to device firmware and cryptographically signing firmware to prevent malicious software from being placed on devices are also easy to implement—but discouragingly rare.

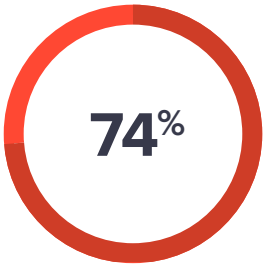
Security researchers like Billy Rios of the firm Whitescope have shown how easily available firmware can provide a roadmap to would-be device hackers and sophisticated nation-state actors.



OF DEVICE MAKERS WHOSE DEVICE WILL EMPLOY SECOND-FACTOR AUTHENTICATION



OF SMART HOME AND SMART COMPANIES EMPLOYING SECOND-FACTOR AUTHENTICATION



OF INDUSTRIAL FIRMS EMPLOYING SECOND-FACTOR AUTHENTICATION

EVENTS LIKE THE PETYA WIPER MALWARE ATTACK in Ukraine—which began with a malicious software update—underscore the risk that vulnerable software supply chains pose. Still, such security features are in the minority among our survey respondents. Just 44% of respondents said they would restrict access to firmware updates on deployed IoT devices, and only 43% of respondents said they would cryptographically sign software or firmware updates. Clearly, this is an area where more explanation and coaching is warranted.

REASON FOR OPTIMISM

Still, there is reason for optimism that device makers are headed in the right direction when it comes to designing security into the connected devices and that—at least among the organizations represented by our respondents—the next generation of connected devices will not repeat the security sins of earlier generations.

DEVICE MAKERS INVESTING IN STRONG AUTHENTICATION

For example, when asked about the kind of security features deployed devices will sport, a whopping 73% said that their device will employ a strong second factor for authentication, such as a one-time password or smart card. That includes 80% of smart home and smart business companies and 74% of industrial firms who took the survey. Those are big numbers and suggest that companies are taking device authentication challenges seriously.

Respondents said their company would apply layered authorization for their devices, with distinct user roles and the principle of “least privilege” (i.e., you get only as much access as you need) applied. Overall, 52% of respondents indicated that layered authorization was on their feature list or already used in their products. Within the industrial and life sciences sectors, the percentage was even higher (54% and 58% respectively).

Likewise, a majority (53%) of respondents said that their company’s connected devices will enforce strong passwords for both users and

KEY POINT

Manufacturers and other device makers have recognized that partnering to deliver critical but complex functionality like user and role management, device attestation, software updates, and device management is the best path to success.

administrators when deployed. Among respondents from consumer electronics and smart home or smart business product firms, that number was even higher—closer to 60%.

INTEREST IN OVER-THE-AIR SOFTWARE UPDATES

Over-the-air (OTA) software updates that are pushed to devices rather than requiring device owners to obtain and then apply updates are another feature that can greatly improve the security of deployed and connected devices. There, also, the survey shows reason to be optimistic, with 40% of respondents indicating that their deployed products will support automatic, OTA updates. Fivety-five percent of respondents from companies in the consumer electronics space said that OTA updates would be supported. Also interesting: it was respondents from companies who had already deployed connected products who were the most interested in OTA update features—which is perhaps an indication of a maturing understanding of the risks facing deployed, connected endpoints.

> ...device makers are acutely aware of the need for proper risk and threat assessment during the product development phase.

Together (and if true) these responses indicate that device makers, even as they pass over important security improvements, are at least embracing proven security measures in areas like device authentication that will pay dividends in years to come.

PARTNERS A KEY FOR IDENTITY, ACCESS MANAGEMENT

So, did our survey of professionals working at device makers convince us that this is happening? In other words, did it show that security investments are aligning with risk? The picture is mixed. In a series of questions, we asked the professionals who took our survey to discuss the steps their organization was taking to develop a secure connected product. We also asked them about the specific technologies they planned to use to secure their devices in deployment.

What we learned from the response to those questions was that device makers are acutely aware of the need for proper risk and threat assessment during the product development phase. For example, asked to rate the importance of risk assessment to the development process, 60% of respondents rated it “extremely important,” while 32% rated it “somewhat important.” Respondents rated threat identification and vulnerability assessment as similarly high priorities for developers.

That’s good news, especially when combined with the findings of earlier questions about developer priorities that identified security and stability as top considerations overall for connected device firms. Furthermore, when we asked our respondents about their plans to address specific security weaknesses such as identity and access management, they indicated that they were addressing the need to secure access to devices.

For example, more than half (56%) indicated that they would be using a third-party Connected Product Management (CPM) platform like LogMeIn’s Xively, Microsoft Azure or IBM’s Bluemix to deploy and securely manage connected devices. In fact, CPM platforms were the top choice of respondents, above traditional public

> ...more than half (56%) indicated that they would be using a third-party Connected Product Management (CPM) platform like LogMeIn's Xively, Microsoft Azure or IBM's Bluemix to deploy and securely manage connected devices.

key infrastructure (PKI) deployments—internally managed (52%) or externally managed (47%)—as well as open standards like The Fido Alliance (34%). Interest in CPM platforms was particularly strong among C-level respondents (60%) and among respondents working for firms in the smart home and business sector (59%) and the consumer electronics space (57%).

CPM platforms were also a popular choice to manage user roles and identities. Around 46% of respondents indicated that they use or plan to use a platform like LogMeIn's Xively to manage user identities for connected device deployments. A similar percentage said they would look to IT asset management tools like those by Kaseya or Solarwinds to handle that task, while traditional identity and access management platforms like those by Oracle, Microsoft or CA were the top choice (51%) for managing user identities in IoT deployments.

At first glance, these results dovetail with other research that suggests device makers are relying on technology partners and ready-made platforms to help launch smart, connected Internet of Things products. Compelled by a lack of expertise internally, manufacturers and other device makers have recognized that partnering to deliver critical but complex functionality like user and role management, device attestation, software updates, and device management is the best path to success—and one that allows device makers to focus on high-value areas like customer relationship management and support.

However, what is clear from our survey is that IoT firms are also in need of partners who can address specific security needs, though they may not fall neatly into an existing product category.

For example, in response to our question about what tools they planned to use to manage user identities, more than one-third (36%) said they planned to use a custom-developed system to do so—a comparable share to those who said a CPM or IT asset management (ITAM) product would be their choice.

Writing your own solution is never a company's first choice. In fact, Xively research has found that 81% of companies attempting to implement an IoT device

on their own end up with cost overruns or with finished products that fall short of security best practices. So, given the high cost, challenges and potential pitfalls of internally developed identity management solutions, what can explain the strong appeal of custom-developed solutions?

One explanation may be that companies aren't finding the features for configuring and managing user access that their device deployments demand in existing products. It's possible that the particulars of IoT deployments fall between the lines of products like identity and access management, CPM, and ITAM suites and services.

An equally possible explanation is that device makers and would-be device makers don't have a well-enough-defined understanding of their product's ecosystem to say what parts they will own and which they will source to others. In the case of identity and access management, for example, this question may reveal that there isn't a clear understanding of the challenges and requirements of managing identity for deployments of smart connected products. That might compel respondents to adopt an "all of the above" approach to the various options for managing user identity and access.

This explanation would jibe with other recent surveys of executives and architects working on connected products. For example, the consulting firm McKinsey surveyed[2] 400 managers in the U.S., U.K., Germany and Japan and found that only a small minority (16%) felt their company was ready for the security challenges of the Internet of Things. Among the factors that came into play were unclear lines of responsibility.[1] "There needs to be a holistic cybersecurity concept for the entire IoT stack," according to the report released by McKinsey. "But often no single player feels responsible for creating it."

As the rise of "thing" botnets like Mirai, Brickerbot and Persirai prove, insecure devices already pose a threat to the stability of the Internet, with many of the security problems linked back to weak authentication schemes. That means controlling and managing access to networks of things is a top priority for devices of all stripes, from plant floor equipment to IP-enabled cameras monitoring a home owner's backyard. However, IoT deployments present new challenges that require a reassessment of features such as network connectivity, device

management, communications security and data security that are wholly different from older generations of IT products.

While its always possible to cultivate these skills and expertise internally, IoT-platform-as-a-service and third-party providers are critical to helping companies accelerate development without sacrificing the security of the finished IoT product.

2. http://www.mckinsey.com/global-themes/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age

Conclusion

Clearly, our survey gives us reason for optimism that the coming generation of connected devices will mark a vast improvement over the balky and insecure nanny cams, digital video recorders and connected appliances that have made up the first generation of the Internet of Things.

KEY TAKEAWAYS

- Security and stability of devices are top concerns.
- Companies are embracing a range of security features that stand to vastly improve the integrity of deployed, connected endpoints.
- Respondents seem preoccupied with remote, external attackers and the risk of data theft, while downplaying the role that product weaknesses play in security incidents.
- More work and education needs to be done to bring device makers across industries up to speed on the most prevalent risks facing deployed devices.
- Partnering with qualified and knowledgeable firms can be one way to bring that needed expertise on board quickly and help safely negotiate this fast-changing landscape.

RESPONDENTS TO OUR SURVEY, representing a broad swath of industries and roles, tell us that the security and stability of their devices are top concerns, and they show a willingness to tackle difficult design and deployment issues, such as authentication and identity management.

Partnering with third-party providers, including CPM vendors like LogMeIn's Xively, is seen as a way to tackle thorny device identity, access and management challenges that IoT deployments entail.

We see, also, that companies are embracing (or ready to embrace) a range of security features that stand to vastly improve the integrity of deployed, connected endpoints. Multifactor user authentication, layered user roles and applications of "user least privilege" as well as the embrace of OTA software updates for devices all rated well with our survey respondents—that's a promising sign.

Still, there is reason for concern. Too many of our survey respondents seem preoccupied with remote, external attackers ("hackers in hoodies," if you will) and the risk of data theft, while downplaying the role that product weaknesses play in adverse IoT security incidents. Often, respondents awareness' of IoT risk seems to diverge from their embrace of features to ameliorate those risks.

In just one example, customers rate theft of personally identifiable information from devices as a top concern, but only a minority say that their company will encrypt communications to and from deployed IoT endpoints. Similarly, less than half of respondents indicated that their company's connected device would mandate changes to default administrator credentials, even though default credentials were the main "infection" mechanism used by the Mirai botnet.

Clearly more work and education needs to be done to bring device makers across industries up to speed on the most prevalent risks facing deployed devices and the best ways to address those risks during design, testing and deployment of connected endpoints. Partnering with qualified and knowledgeable firms and leveraging proven platforms and service providers can be one way to bring that needed expertise on board quickly and help safely negotiate this fast-changing landscape.

XIVELY ACCELERATES YOUR IOT JOURNEY

Xively has an established record of successfully helping customers get to market with IoT-connected products.

Xively, the IoT division of LogMeIn, works with companies around the world to bring to market the most successful and innovative IoT products available today.

Xively's CPM platform helps companies connect products securely, manage connected products and the data they produce, and reimagine how they engage with their customers.

xively™ by LogMeIn

320 Summer Street
Boston, MA 02210
866-478-1812
XivelyInfo@LogMeIn.com

XIVELY.COM