Identity and Access Management:

A Challenge that Never Gets Old, But Sure Gets Harder

Dr. Thomas P. Keenan, FCIPS, I.S.P., ITCP, University of Calgary

in collaboration with

Ron Murch, I.S.P., ITCP, University of Calgary

In partnership with: FORTINET

Identity Access Management White Paper—August 2020

Introduction:

IN 1971, HOW DID TOM KEENAN PROVE THAT HE WAS AUTHORIZED TO USE A CERTAIN MAINFRAME COMPUTER? SIMPLE: HIS BOSS HANDED HIM THE KEY TO THE AIR-CONDITIONED LAIR OF THE IBM 360/50 AND INSCRIBED HIS TIME SLOT, "SUNDAY MORNING 2-4 AM" ON THE BLACKBOARD BY THE DOOR. TOM ALREADY KNEW WHICH CONSOLE BUTTONS TO PUSH, AND WHICH *NOT* TO PUSH!

Dr Thomas Keenan (left)

Ron Murch (right)

Even earlier, in the summer of 1968, while studying at the University of Waterloo, Ron and his fellow undergraduate students had unfettered access to the IBM System 360/75 installed there. Any night, they could walk in, access "the fishbowl," operate it themselves, and run whatever programs they felt they wanted to.

No login required, no pesky passwords, and no audit files tracking what these early computer users did on their "booked time".

Then, along came time-sharing services, passwords, minicomputers, microcomputers, bad passwords, hackers, data breaches and Wikileaks. Not to mention the Internet and "The Cloud", whatever that means to you. Data became more valuable while at the same time it got much harder to figure out who was on the other end of that connection – is it Friend or Foe?

In May and June 2020, the CIO Association of Canada (ciocan.ca) convened some of Canada's top experts in information security for a series of frank online discussions. These programs were under the Chatham House Rule, so speakers (except for the two presenters) are not identified by name or title. Still, we can peek over their shoulders and benefit from their considerable wisdom.

The sessions were led by Derek Manky, Chief of Security Insights for FortiGuard Labs; and moderated by Bobby Singh, CTO and Chief Information Security Officer (CISO) for the TMX Group. In these three wide-ranging videoconference conversations, an elite group of Canadian CISOs tackled the pressing issues in Identity and Access Management (IAM), especially as it applies to the Business Risks, the Internet of Things and 5G technology.

Everyone agreed that the complexity of IAM went up considerably when COVID-19 forced us to hunker down and work from home. This *modus operandi* is certainly safer for people, but what about for our IT systems and the valuable data they hold? Are there increased risks? What are they?

Many organizations, private and public, had to turn on a dime as they sent their employees home for an indefinite period. Even if they were already planning to be "digital-first" or "fully digital", the pandemic vastly accelerated this transformation, with security sometimes being an afterthought.

WHAT IS IDENTITY?

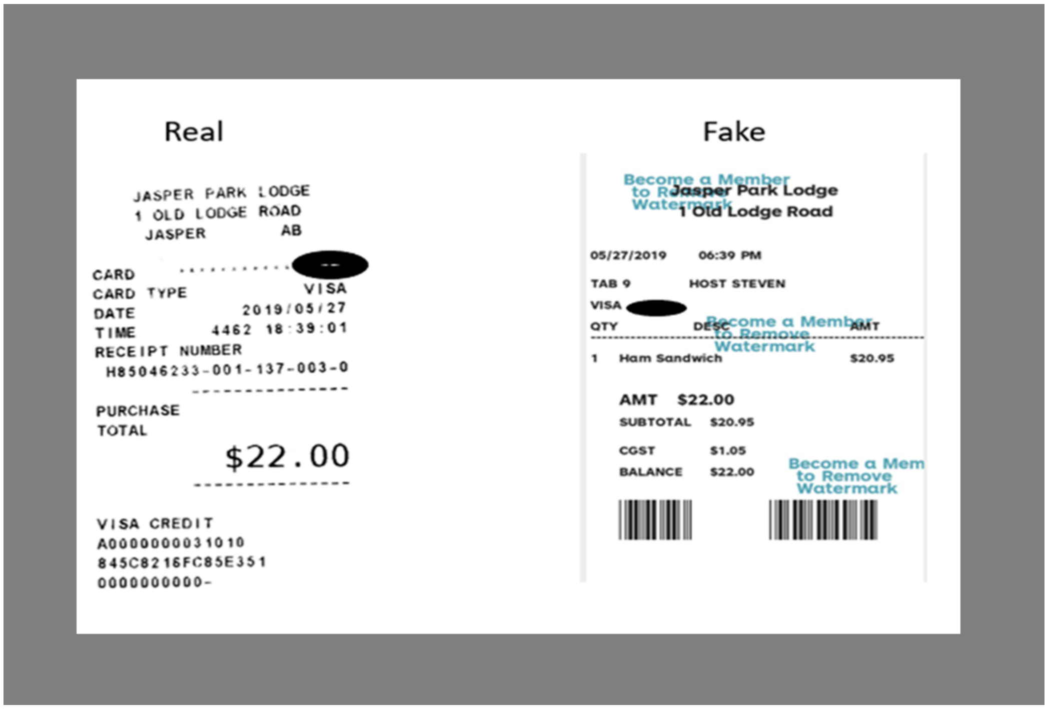
Identity is often associated with a human being. However, it can be applied to other entities such as a business partner organization, a supplier's automated inventory replenishment system, even an online shopper who hasn't been fully identified yet. Identity may even be constructed dynamically, as we learn more about who is on the other side of the connection.

The retail chain Target builds an identity for each new potential customer starting with "we've just seen this debit card that we haven't seen before". This is then augmented with purchase history, and even home and email addresses if the customer provides them. This led to the famous (and controversial) "Target knows teenage girl is pregnant before her father" *New York Times* story[1].

Corporate directories on a website are a goldmine for obtaining identity and corporate structure data, and postings on LinkedIn can lead the bad guys to the person who can authorize a payment.

We've all heard about identity theft as it applies to individuals, but corporate identity is also easy to steal. I was just able to download high-resolution logos for all of Canada's major banks with a simple Google search on "logo bankname". It's a small step to faking up a bank statement or official-looking letter, or whatever else you want.

Dr. Tom Keenan presented a paper at the recent Hackers On Planet Earth conference[2] in which he magically morphed a receipt for two beers at the Jasper Park Lodge into a ham sandwich -- for expense account purposes. Of course, since he was speaking to a conference of judges there, and they don't reimburse the cost of alcohol, he never submitted that bogus receipt!



Real

```
   JASPER PARK LODGE
  1 OLD LODGE ROAD
    JASPER          AB

CARD          ...........[redacted]
CARD TYPE                  VISA
DATE                 2019/05/27
TIME            4462   18:39:01
RECEIPT NUMBER
 H85046233-001-137-003-0
            ---------------
PURCHASE
TOTAL
               $22.00
            ---------------

VISA CREDIT
A0000000031010
845C8216FC85E351
0000000000-
```

Fake

```
        Jasper Park Lodge
         1 Old Lodge Road

05/27/2019     06:39 PM

TAB 9          HOST STEVEN

VISA [redacted]
QTY            DESC                AMT
---------------------------------------
1   Ham Sandwich                 $20.95

    AMT   $22.00
    SUBTOTAL   $20.95

    CGST       $1.05
    BALANCE    $22.00
```

THE DANGERS OF SHODDY IDENTITY MANAGEMENT

Business Email Compromise (BEC) is the simple act of impersonating someone via email to make something happen – usually a large fraudulent wire transfer. Victims are often reluctant to talk about their identity breaches – it doesn't speak well of their internal practices and controls. But it's definitely real – and, it's all about money!

A Calgary senior citizen was tricked into wiring $619,000 U.S. to a scammer. The victim didn't notice two letters transposed in a domain name, perhaps because he was so excited to be buying a condo in California. Instead, he wound up sending the money to a fraudster in Colorado, who rapidly moved it to China. The victim is suing his own bank for honoring the transfer, saying that they should have prevented it.[3]

On a happier note, Edmonton's MacEwan University managed to recover most of the $11.8M that was deliberately mis-directed to an external bank account. They thought they were paying the construction firm that did on-campus projects. Media reports say the purloined funds were traced to a bank account in Montreal and to two accounts in Hong Kong, which were frozen.[4] They still came up $900,000 short, prompting the Minister of Advanced Education to direct all Alberta universities to review their financial controls.

In the CIO Association discussions, one CISO observed that everybody is getting increasingly paranoid about emails and sometimes legitimate ones are treated as suspicious. Several companies noted that they flag emails that come from outside their organization, though this could still be subject to hacking – e.g. if the bad guys are crafty enough to tamper with an organization's Microsoft or Azure Active Directory.

Like "The Boy Who Cried Wolf", tightening up corporate email practices can have unintended consequences. One CISO reported problems using surveys from SurveyMonkey because people doubt the authenticity of emails from external sites. Putting links to surveys up on a corporate Intranet was suggested as one solution. Also, you can use verified internal emails to alert employees that a survey will be coming their way.

"Hey, Larry did you send this?"

Another participant mentioned that his company has a single point of approval (the CFO) for all wire transfers, ideally backed up by a phone call. In several cases, this simple precaution has averted a large, fraudulent cash transaction. In one instance, the recipient of the phishing email happened to be working in the same room as the person who allegedly requested the transfer. He was able to lean over and ask something like "Hey, Larry did you send this?"

Participants in the sessions all agreed that humans are the weakest link in many systems. The bad guys are seeking money, and also valuable data or information that can be sold or mis-used. Health records are particularly prized as they usually contain enough information to carry out identity theft.

Privileged access is an important IT management capability and is a perennial issue since somebody has to be able to open or close that pipeline valve, enter cheque requisitions, and do all the normal functions of a business. Targeted emails ("spearphishing") are a popular way to try to compromise a system, and often its associated network.

Phishing test campaigns are becoming popular, with appropriate feedback to people who click on bad links. One firm reported that if somebody fails their phishing test "we lock their account, and force them to change their password, and this has changed user behavior".

Lawyers are a particular target of spearphishing because they often provide detailed personal credentials and contact information on their law firm's website. This makes it easy to craft emails that appear to come from a partner or an associate in the firm. Also, there are vulnerabilities when they deal electronically with clients. These range from man-in-the-middle attacks to destination compromises, perhaps, as one participant noted, at "that cannabis company that doesn't have a good I.T. department".

WHO'S ON THE OTHER SIDE?

Cybercrime has changed mightily since 1986 when Clifford Stoll detected a 75-cent anomaly in computer billing records and launched an investigation that culminated in his wonderful book *The Cuckoo's Egg*.[5] That detective work took a very determined Stoll over ten months, part of it spent trying to convince skeptical law enforcement officials to take an interest in such a small amount of money.

"The bad guys even have affiliate programs,"

Hunting hackers is a full-time job name for cybersecurity pros like Derek Manky. He notes that hacking is also a business for the people on the dark side of cybercrime. "The bad guys even have affiliate programs," he laughs. "At FortiGuard Labs' we are also trying to find the identities of the cybercriminals." He says they've had some success, uncovering one crime organization with "four different groups totaling 46 employees, who were running "419 scams", romance scams, but the biggest thing was payment diversion fraud. They were intercepting accounts payable invoices and forging SWIFT bank codes. They were able to steal about $61 million over three months."

The bad guys are driven by two main motivations, money and reputation among their peers. They have all sorts of tools at their disposal to thwart our defenses. "It's very cheap for cybercriminals to do things like spoof IP addresses, changing them 5 or 10 seconds later. So blocking by IP addresses doesn't work anymore." Manky advocates a much more active approach and notes that "I don't think there's ever going to be a silver bullet." Nor will there be a one size fits all approach. The Cloud has certainly made identity management more complicated, especially for organizations that use multiple cloud service providers. Manky mentioned that he's on an INTERPOL working group on cybercrime and that inter-agency co-operation is becoming even more important.

COVID-19

Allowing people to work from home was always a challenge, even more so in a crisis – and especially during the COVID-19 crisis, because companies had to transition to remote workforces literally overnight! “We’re always at a disadvantage since cybercriminals can adapt quickly.” There are reports of how quickly they pivoted when COVID-19 struck, taking advantage of the fact that people were working from home and could be more susceptible to a bogus “please send a wire transfer today” email that looks like it’s from the boss. It’s kind of BYOD to the max since some people are using computers at home that are shared with other family members, who may not practice good cyber-hygiene. Telework makes the need for multi-factor authentication even more critical.

One attendee noted that his company has “sped up our project to get rid of our VPN,” moving instead to SaaS. There was a consensus that the job of the CISO is getting more and more complex – and cybersecurity is now also being better recognized at the Board of Directors level as a critical element of business risk that merits deliberate attention, funding, and management.

ARTIFICIAL INTELLIGENCE

We’re seeing criminals now using AI tools to target their spearphishing campaigns, and also doing more “vishing” (voice phishing). In the U.S., the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint security advisory[6] in August 2020 about this problem, noting that "The actors used social engineering techniques and, in some cases, posed as members of the victim company's IT help desk, using their knowledge of the employee's personally identifiable information—including name, position, duration at the company, and home address—to gain the trust of the targeted employee."[7] They also “registered domains and created phishing pages duplicating a company’s internal VPN login page, also capturing two-factor authentication (2FA) or one-time passwords (OTP)” according to the FBI/CISA warning.

“To respond we’re developing playbooks at FortiGuard Labs’ ,” says Manky, “focusing on the attribution of the cybercriminals, right down to their handles, phone numbers, etc.” In response to a question about whether there will ever be a purely technical solution to cybersecurity, Manky opined “I don’t think there’s ever going to be a silver bullet. There will always be people involved, but there are often gaps that we can find and try to plug.”

INTERNET OF THINGS AND SCADA SYSTEMS

Manky reported that “we [FortiGuard Labs] monitor 100 million threat events per day. For the last five years, the top six of ten threats on a daily basis are IoT related – printers, off-the-shelf routers, IP security cameras, etc. Unfortunately, hacking these is still quite easy, and they’re used as a springboard for lateral attacks.”

Having secure protocols is not sufficient since “You can have all the secure protocols in the world, but you need to think about analytics from your core network”. The human factor comes in here because of social engineering — smart people attack people instead of banging their heads against security technology. One participant noted that “the weak link is always the user…Our biggest risks always come from within, somebody going where they shouldn’t be going, not following process, clicking on an email.”

There are many examples of well-meaning people not thinking about the consequences of their actions. An excellent example involved a prison access control system that was designed to be highly secure and have no Internet connection. It used PLCs for functions like door control and was supposedly air-gapped from the outside world.

At DEFCON 19 in 2014, Tiffany Rad and her associates described doing security audits on prisons. “Some of the stuff we found was surprising,” she reported. “If there’s a commissary or food vendors, those have a lot of Internet connections. We were able, in one circumstance, to trace that network to the (prison door) control room. You shouldn’t be able to get from the commissary to the control room.”[8]

One CISO opined that “I don’t think we’ll ever get back to an air-gap world, but we can do segmentation and use a defense-in-depth strategy.”

There’s no question that many field devices with IP addresses are being added and they’re generating masses of data. There’s a disturbing tendency to buy the cheapest gear as opposed to some with more vetted security. This could be costly in the long run.

“We definitely need usage analytics from that type of environment,” says Manky, noting that the bad guys always look for the easiest route to compromise a system. “It’s harder to access microwave transmissions than it is to put malware on a device and collect data from the device directly,” Manky noted.

“Some of the stuff we found was surprising,” she reported. “If there’s a commissary or food vendors, those have a lot of Internet connections. We were able, in one circumstance, to trace that network to the (prison door) control room. You shouldn’t be able to get from the commissary to the control room.”

WHAT BECAME OF PUBLIC KEY INFRASTRUCTURE (PKI)?

A decade or so ago, PKI was touted as the ultimate solution for identity management. Now we hear about blockchain. What's best?

One CISO explained that "Our users don't want the complexity of PKI for 99% of what they do. We could be using Signal now and get more security, but it's not ultimately flexible, e.g. if we wanted to move files back and forth or for regulatory compliance." The best answer is to educate users.

The same participant noted that "We're allowing remote access to our corporate network. It requires a laptop created by our IT department and then the users need to provide multi-factor authentication." However, "if users are now remote and responsible for their own security environments, how can there be confidence that the user has not unwittingly compromised our environment by their actions in their own environments?"

5G

When the world fully adopts 5G and uses IPv6 there will be a much different technical security stack built in there. However, we haven't test driven this yet in the real world. It's a double-edged sword. You have devices that connect peer to peer *ad hoc*, and then it becomes a question of how you inspect that. When we get into the world of 5G, it's not going to get easier! We are talking about more devices, quicker speed, more vulnerabilities, and, obviously, more challenges.

We couldn't avoid the question of who should be allowed to build a country's 5G network. Manky took a neutral position but said "if you think about it, any network could be gamed for malicious use. I can tell you (communications technology hardware) companies like that will have a lot of data so there's always going to be an arm or a connection."

It was also noted that a malicious actor could conceivably do a remote denial of service attack on a country's 5G infrastructure. A poll of the group on the question "Should Canada allow Huawei to build parts of its 5G infrastructure?" resulted in 75% of those voting saying "no".

SWARMBOTS AND HIVENETS

This involves swarms of intelligent bots that communicate with each other in real-time to attack systems. They can get information from specialized search engines like Shodan, which looks for open ports and services. It's definitely a threat on the horizon to worry about. Defence requires shared, actionable intelligence between security solutions. Derek Manky did an entire presentation on this subject at RSA 2018.[9]

ZERO TRUST MIGHT BE THE PATH TO FOLLOW

Zero Trust has been getting a lot of press lately and experts agree that it is poised for an increasing role in our cybersecurity battles.[10]

One of the CISOs summed up the situation as follows:

"I've been pushing zero trust for a couple of years and it's a challenge to get buy-in at the executive level but now people see what zero trust could do. Now, we have 30 % of our workforce effectively on zero trust because they are using cloud services. It works so much more effectively than having to get them into [our] corporate network."

The same participant noted that "Travelling people have a radically different experience. I'm trying to get to a consistent experience no matter where you are. As soon as I moved to Office 365, we built in micro-segmentation, and we're looking at zero trust for everybody. We'll be off data centres and I hope also our corporate network in two years."

Another CISO noted that their company is "cloud-native" and so zero trust is part of their standard operating practices.

CONCLUSION:

One consensus that emerged from these sessions is that technology alone will not fully address our current and future challenges. Good cybersecurity has a strong social component – we can leverage technological capabilities to help us and our data “stay safe and secure,” but the reality is that each individual needs to have a good, well-informed appreciation of the risks and know how to minimize them. Regular, consistent, and credible education is becoming standard practice. This extends to all levels of the organization – hackers have been known to extract critical information from casual chats with the receptionist.

The second thing that became clear is that there is great value in this kind of “off-the-record experience sharing” with peers. Most of the attendees attended all three sessions and participated actively. Knowing that their comments would not be attributed back to them allowed them to ask and answer questions quite freely – and, perhaps most importantly, share both their concerns and their organizational practices while getting help and perspectives from their peers.

Finally, we all gained an even greater appreciation that the job of a CISO is a unique mixture of being able to understand technical issues, appreciating how quickly situations can change, and, most of all, being able to deal with the most complex computers on earth – the human brains of our co-workers.

There’s a lot more processing power, and unpredictability, in that grey matter than all the IBM 360s ever manufactured.

REFERENCES:

1. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#6f4e29af6668

2. https://archive.org/details/hopeconf2020/20200730_1700_Fakes_Aren't_Funny.mp4

3. https://www.cbc.ca/news/canada/calgary/wire-fraud-email-condo-sale-1.5358363

4. https://globalnews.ca/news/4122937/macewan-university-recovers-millions-lost-in-phishing-scam/

5. https://www.wired.com/story/meet-the-mad-scientist-who-wrote-the-book-on-how-to-hunt-hackers/

6. http://www.documentcloud.org/documents/7041919-Cyber-Criminals-Take-Advantage-of-Increased.html

7. https://www.zdnet.com/article/fbi-and-cisa-warn-of-major-wave-of-vishing-attacks-targeting-teleworkers/

8. https://www.youtube.com/watch?v=t2HDFNzqZvk

9. https://www.rsaconference.com/industry-topics/presentation/order-vs-mad-science-analyzing-black-hat-swarm-intelligence

10. https://www.techrepublic.com/article/zero-trust-is-critical-but-very-underused