AUTHENTICATION
WHO ARE YOU AGAIN, AND WHY DO I NEED TO KNOW?

Mark G Graff
Founder & CEO
Tellagraff LLC

ECC 2016

Marist College

13 June 2016

“Life
is not
one damn
thing
after
another.

It is the
same damn
thing
over and
over.”

Edna
St. Vincent Millay

AGENDA

- One traditional model of security
- One pivotally bad year for security
- Two instructive recent catastrophes
- Two promising innovations in authentication
- Three illustrative use cases
- One conclusion

TRADITIONAL SECURITY MODEL

- Traditional security steps
  - Identification
  - Authentication
  - Authorization
- Traditional keys to Authentication
  - “Something you know”
  - “Something you have”
  - “Something you are”

MAJOR INCIDENTS REPORTED IN 2014

- **Target.** Hackers stole names, mailing addresses, phone numbers and email addresses from over 70 million shoppers, and credit card information of 40 million shoppers. Initial access used credentials stolen from HVAC vendor via phishing.
- **Home Depot.** Hackers infiltrated in April, putting 56 million accounts "at risk". Initial entry was via stolen third-party credentials, then point-of-sale (POS) devices were compromised via a Microsoft Windows vulnerability.
- **JP Morgan Chase.** The entry vector (indirectly) was a website built and maintained for JPMC by a third-party vendor in support of a charitable footrace. Usernames and passwords for 76 million households, 7 million small business accounts stolen.
- **Sony.** Hundreds of hard drives wiped, millions of emails stolen and leaked, six unreleased films in digital format leaked. Attack attributed to North Korea as response to the movie *The Interview.* Initial vector: spear phishing.

Sources: Heritage.org, SC Magazine, Krebs on Security, personal knowledge

CYBER APOCALYPSE: OPM DEBACLE

- Two cyber breaches of the Federal Office of Personnel Management were disclosed in June 2015. Together they represent the most significant cyber breach in history
- The first-announced attack yielded primarily "PII" Personally Identifiable Information on over 4 million current and former federal employees, including Social Security number, home address, birth date, job and pay history, gender, and race. This loss meant China could:
  - Build a fully staffed functional map of our federal operations.
  - Unleash, at will, a flood of identify thefts, impersonations, and break-ins to personal accounts using pilfered information.
- The second breach compromised the complete federal database of answers to Form SF-86, the 127-page long Questionnaire for National Security Positions. The form is specifically designed to uncover potential topics of blackmail. The personal records of about 21.5 million persons were stolen.
- The Chinese now hold intimate and potentially damaging information on about 22.1 million Americans deeply involved in our national intelligence and security operations and policies, the theft of the SF-85 database must be considered one of the greatest intelligence defeats in history.
- As Sun Tzu wrote in The Art of War, "The supreme art of war is to subdue the enemy without fighting."

Sources: Washington Post, Krebs on Security, personal knowledge

- Over 11,000 financial institutions worldwide use the SWIFT system to move funds internationally
- Ecuadorian bank lost $9M in January 2015
- Vietnamese Tien Phong bank attacked in December 2015
  - Intercepted an attempt to remove $1.1M using an outside vendor's infrastructure.
- Bangladesh central bank, $81M stolen February 2016
- October 2015 attack on a bank in the Philippines also rumored
- Symantec has publicly linked SWIFT attacks to the 2014 SONY attack, (malefactors nicknamed "Lazarus") and hence the North Koreans.

SUDDENLY, A CENTRAL CONCERN: THE "SWIFT" INCIDENTS

1. The users clicked on spear phishing emails
2. The users had weak passwords
3. CISO relied on the security of the supply chain
4. CISO neglected Point of Sale devices
5. CISO did not understand the network topology
6. Enterprises relied on flawed open source software
7. Enterprises put up websites vulnerable to SQL injection
8. Enterprises did not properly segment their networks
9. Enterprises put too much faith in technology sold to them

OPM: 1, 2, 3, 5, 8, 9, and many (most?) others

SWIFT: 1, 2. 3, 8, 9, variant of 4, and others

THE MISTAKES BEHIND RECENT CYBER EVENTS

"Out of the crooked timber of humanity no straight thing can ever be made."

Immanuel Kant

What factors influence our decisions whether to trust someone or be afraid of them?

- Many factors we observe seem suited to the African savannah
  - Distance/proximity
  - Signs of aggression/posture/bared teeth
  - Apparent similarities to us
- Society enforces structures of accountability, often across borders
- Effect: aggression is often predictable and discernible, and often has consequences

- Yet on the Internet:
  - Distance is irrelevant
  - Aggression can occur transparently, under our radar
  - Appearance is malleable and identity largely unverifiable
- Society unevenly enforces accountability, especially across borders
- Effect: Aggression can be unpredictable and consequences negligible

IMPLICATIONS OF THE SIMIAN RISK MODEL

- Phishing compromises mean that authorized, authenticated users are effectively executing the attack
- Requests for access from tens of billions of potential connection sources are given equal weight
- Attackers now routinely shape-shift in identity, IP address, malware, and other ways to circumvent black-listing methods in several dimensions
- Access requests that would never be considered rational by human agents are routinely honored if technical policies are observed

The challenge is to make as much use of *real-world common sense* as possible in cyber space, while avoiding our "simian" blind spots

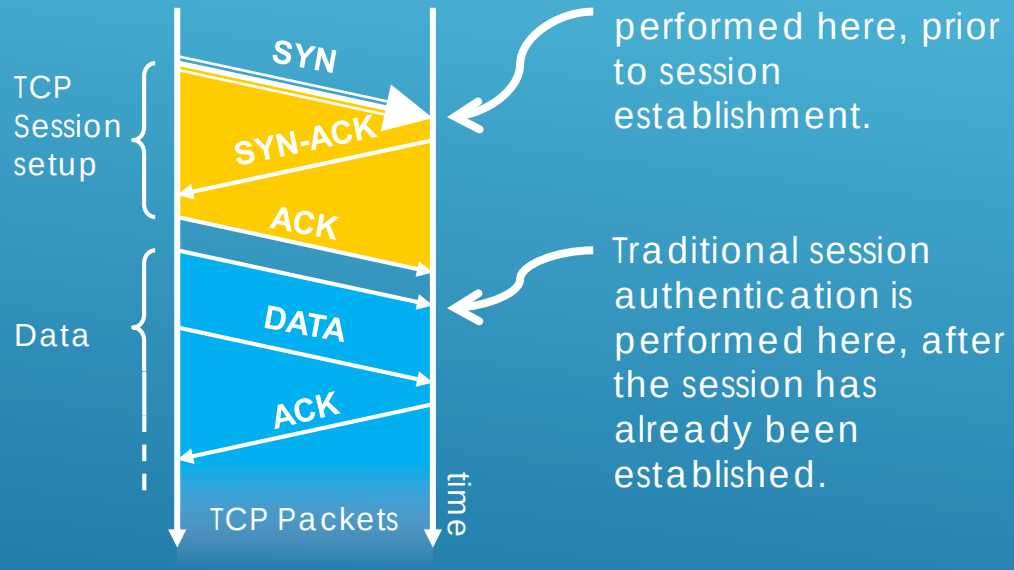
FLAWS IN TRADITIONAL AUTHENTICATION

- The company BlackRidge Technology offers ”First Packet Authentication™” (FPA)
- FPA incorporates non-interactive authentication protocol into existing TCP protocol
  - Engages on first packet
  - Preserves compatibility with existing network, security, identity and application infrastructure
- Operates using cryptographically secure Identity Tokens
  - Very efficient; fits into TCP header without frame expansion
  - Address and topology independent, supports dynamic addresses and NAT

BlackRidge TECHNOLOGY

AUTHENTICATION VIA “FIRST PACKET”

Transport Access Control (TAC) Authenticates every TCP session request before responding and establishing the session



BlackRidge TECHNOLOGY

TRANSPORT ACCESS CONTROL

AUTHENTICATION VIA ASSURED PLACE

- The company Digital Authentication Technologies (www.dathq.com) offers an element that's been missing from classical authentication:
  - Contextual Location Fingerprint" (CLF) offers *strong authentication of location*
  - **"Someplace you are"**
- CLF collects and compares data about a location that can only be obtained inside its environment (e.g., unique RF measurement)

ILLUSTRATIVE USE CASES

- These two astounding technologies, TAC and CLF, offer new opportunities in many use cases. Examples:

1. Secure virtual enclaves
2. Geographically dispersed critical operations
3. Software distribution

SUMMING UP

- Traditional authentication methods are dangerously inadequate today
  - Based on technological ease of implementation
  - Chiefly rely on blacklisting approaches
  - Authorize requests human agents would find ludicrous
- I endorse two innovative technologies:
  - Digital Authentication Technologies offers CLF authentication based on “Some place you are”
  - BlackRidge Technology offers First Packet Authentication, the *earliest intervention possible* on any network request.
- We desperately need authentication methods, like these two, that can be tied to the same factors humans would use In Real Life but avoid our “simian” shortcomings – and that can operate to scale.

“Learn all you can from the mistakes of others. You won’t have time to make them all yourself.”

Alfred Sheinwold

BACKUP SLIDES

SHORT REVIEW OF MY CAREER

- Wrote first program (in BASIC) in 1966
- Entered Information Technology in 1975, repairing computers for USAF
- B.S in Computer Science, USM 1978
- Job highlights:
  - Security coordinator/architect for Sun, 8 years
  - CCSO for LLNL for 9 years
  - CISO for NASDAQ for 3 years
- Major software projects:
  - Network “Policy” program, TOPS-20, 1984
  - Security system for Louvre, other museums 1986-1987
  - Control interface for nuclear reactors, ATM’s 1990-1991
  - Stealth search for scattered information, 2010-2011
- As of 2016: 50 years of programming, 41 years in IT, almost 30 in security

- Breach occurred in November 2013, announced in January 2014
- Initial access was on 15 November using credentials stolen from Fazio Mechanical Services, an HVAC provider, via phishing
  - Connection between Fazio and Target was for “electronic billing, contract submission, and project management”
- Next step was to install malware on a small number of cash registers
- Final stage: infection of majority of point of sale devices
- Hackers stole:
  - Names, mailing addresses, phone numbers and email addresses from over 70 million shoppers
  - Credit card information of 40 million shoppers (later sold for $53.7M)
- CEO resigned, other executives summoned to testify before Congress
- Estimated cost to Target range from $148 million up to $420 million

Sources: Newsweek, Krebs on Security

MAJOR 2014 INCIDENT: TARGET

MAJOR 2014 INCIDENT: HOME DEPOT

- Home Depot confirmed in September that they had been infiltrated by hackers since April
- 56 million accounts were ”put at risk”
- The company expected to pay $62 million to cover the costs of the attack, including legal fees and overtime for staff, and causing an estimated $90 million in costs for banks to replace 7.4 million debt and credit cards.
- Unnamed staff within Home Depot said that the company’s information security department struggled with high turnover and old software.
- The team resisted using the Endpoint security feature of Symantec’s cybersecurity program, a feature that tracks and alerts system administrators of suspicious activity, despite the urging of security consultants.
- The company also did not encrypt customer card data until September 2014.

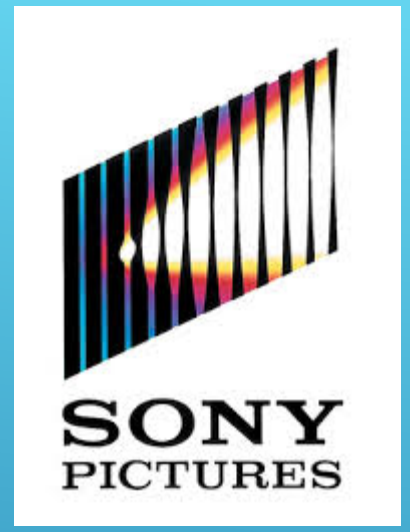
Sources: Newsweek, Krebs on Security

MAJOR 2014 INCIDENT: J.P. MORGAN CHASE

- In August, the networks of J.P. Morgan Chase, were infiltrated by a network of hackers. The attack went unnoticed for two months.
- The entry vector (indirectly) was a website built and maintained for JPMC by a third-party vendor in support of the “J. P. Morgan Corporate Challenge”, a charitable footrace.
- Usernames and passwords stolen from that website were used to gain access to other parts of the JPMC enterprise network
- In an SEC disclosure filing on 2 October, J.P. Morgan said that:
  - 76 million households and 7 million small businesses accounts were affected
  - Hackers were NOT able to access the most private data like Social Security or account numbers
- Many experts attribute the attack to Russian cyber criminals; FBI says Russian government was not behind the attack

Sources: Newsweek, Krebs on Security

- It all seems to be about the movie *The Interview*, about a CIA plot to assassinate North Korean "Dear Leader" Kim Jong Un.
- SPE was hit with a strain of malware designed to wipe all computer hard drives within the company's network.
- The attackers then leaked mass quantities of sensitive SPE internal documents (remember the snide remarks about President Obama's film preferences?)
- Later data dumps included more than 25 gigabytes of sensitive data on tens of thousands of Sony employees, including social security numbers, medical and salary information.
- Attackers also dumped onto the Internet digital copies of five hitherto unreleased movies: *Fury*, *Annie*, *Mr. Turner*, *Still Alice*, *To Write Love on Her Arms*,
- FBI, NSA directors directly attribute the attack to North Korea
- FBI Director Comey: Spear phishing emails sent to Sony employees as late as September of 2014 appear to be the "likely vector for the entry into Sony."



Sources: Krebs on Security, SC Magazine, personal knowledge

MAJOR 2014 INCIDENT: SONY PICTURES ENTERTAINMENT

POLICY: THE ILLUSION OF CONTROL

- Assumption others share your concerns and values
- Assumption we understand the environment and the threat
- Assumption your users understand the risks
- Assumption your responsibility entails authority
- Tragedy of the Commons

ANALYSIS: THREE COMMON MISTAKES

- Fallacy of the near
- Fallacy of the Other
- Model blindness