Welcome to SecTor

“Navigating Cyberspace: Identifying A New Path to Defeating Tomorrow’s Attacks”

Solomon Sonya
@Carpenter1010
Disclaimer: The views presented are those of the speaker and do not necessarily represent the views of the United States Department of Defense (DoD) or the US Air Force.
Whoami

- Assistant Professor, Computer Science, United States Air Force Academy
- Research Scholar, University of Southern California, Los Angeles
- Director, Intrusion Response, Air Force Enterprise Computer Emergency Response Team
- Senior Enterprise Network Defense Manager
- Software Reverse Engineer
- Software Developer

Education:
- M.S. Computer Science, Air Force Institute of Technology
- M.S. Information Systems Engineering, Western International University
- B.S. Computer Science, Texas Christian University

Hobbies: Cyber Security, Exploitation, Data Protection, Net Defense Paradigms
Framing the Problem...
Framing the Problem...

- Tomorrow’s attacks may be worse than today...
  - Malware, system exploitation, unintentional data loss continue to increase in prevalence and sophistication

- The security state of an arbitrary protection system is indecipherable  
  (Harrison & Ruzzo “Protection in Operating Systems” - 1976)

  - Weaknesses will always exist even in defense-in-depth deployments

  - Understanding these weaknesses should be the motivation towards designing better security paradigms tomorrow
Understanding the Attack Domain
Updated Anatomy of a Cyber Attack

- Reconnaissance/Research
- Stage Exploits
- Social Engineering
- Scan Targets
- Penetration
  - Privileges++
  - Pivot
  - Pillage
  - Paralyze
- Evade Detection
- Maintain Access

Sources:
- Water-Hole
- Drive-By
- Phishing
- XSS
- Protocols
- Trojan
- Insider
- Hardware
- Embedded Devices
- Active & Passive
- Ping Sweep
- ARP Scan
- Port Knock
- DNS Lookups
- IP Reservations
- Management Protocols

Source: Solomon Sonya @Carpenter1010
SUN TZU

KNOW THY ENEMY, KNOW THYSELF

500 BC   “The Art of War”   Inventor of Agile Warfare
Piloting with a broken compass...

The failure of today’s security paradigms are predicated on a false belief that detection is key to success...

Our systems are almost always patched, firewalled, AV’d, monitored by IDPS - yet attacks continue to increase in prevalence and sophistication...
Brief Evolution of Malware
Brief Evolution of Malware

Slammers (Search && Destroy)

Email and Social Networking propagation (e.g. Ad dispersal)

Ubiquitous Command and Control (e.g. Conficker)

Mobile Resident and Propagating Malware

PUNT!!!

Source: Solomon Sonya @Carpenter1010
Solomon Sonya * @Carpenter1010 * SecTor, Canada * @sectorca  “Navigating Cyberspace: Identifying A New Path to Defeating Tomorrow’s Attacks”

Cell Phones: A data trove for exploitation...

- When was the last time you audited permissions granted to your apps?
- Is all of this necessary to show a light? (I don’t think so…)


Really?!!!

Really?!!!
“At the height of their operations, a [Russian National] hacker arrested last year reportedly used an Android banking trojan [Banks at your fingertips] to steal between $1,500 and $8,000 from victims on a daily basis. With over 2 billion users estimated to access banking services through their mobile devices, cybercriminals see [cell phones] as a data trove they can monetize.”
– TrendMicro 2018 Annual Threat Report

How much security do you apply to your phone that you also use for banking, shopping, surfing, and email transactions?

If I own your email, I can probably gain access to your financial portfolio...
Brief Evolution of Malware

Slammers (Search && Destroy)

Email and Social Networking Propagation (e.g. Ad dispersal)

Ubiquitous Command and Control (e.g. Conficker)

Mobile Resident and Propagating Malware

Data Theft (e.g. Zeus, Duqu)

Point-of-Sale

Ransomware

Hardware Resident Malware (Fileless)

Cryptocurrency-Mining Malware

Living-off-the-Land (LotL)

Source: Solomon Sonya @Carpenter1010
Did you know...

Vendors have tried to say the lifespan of zero-day malware is reduced to only hours from initial discovery...

Independent report by RAND “Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits” had an average life expectancy of 6.9 years. Only 25% did not survive 1.51 years; 25% persisted for 9.5 years
- China’s attack to harvest data across air-gapped networks (removable media). Adapted malware since 2005

- Iran’s wide-spread cyber-espionage attacks on governments, financial, energy, chemical, telecom institutions in the Middle East

- N.Korea’s world wide attacks on Financial institutions

- APT18 - China’s espionage group using malware and phishing campaigns to target Construction, Engineering, Aerospace, governments in Us, EU, JP

- APT10 - China’s espionage group using malware and phishing campaigns to target Construction, Engineering, Aerospace, governments in Us, EU, JP

- APT3 - China’s attack on Aerospace & Defense, Construction & Engineering, High Tech, Telecoms, Transportation industries. Exposed malware, TTPs, C2 infrastructure

- APT1 - 2013 Exposed China’s multiyear (7+) attacks on 141 different industries. Exposed 3k indicators: domains, malware, X.509 certs; malware resurfacing today
Some argue attacks of tomorrow will no longer exist due to advancement in detection and prevention technologies...

But if this is the case, why does the evidence reveal the contrary?

Attacks continue to increase, new malware is on the rise.
Central Malware Evolution Themes...
Central Malware Evolution Themes...

What can I do?
How do I get you to pay me?

How do I move?

How do I thrive?
What can I take to generate money?

How do I communicate?
How do I evolve?
Adjust your view of the World...
Adjust your view of the World...

Were these Cyber Attacks?

Stuxnet
Tomorrow’s attacks will be asymmetric and unconventional in nature...
October 31, 1999 - EgyptAir Flight 990 from Los Angeles, CA to Cairo International Airport, Egypt crashed into the Atlantic Ocean killing all 217 passengers and crew on board. The Egyptian Civil Aviation Agency (ECAA) ruled the crash a result of mechanical failure. US’ NTSB ruled crash apparent suicide by the First Officer…

“Why didn’t he crash it into a building?”
How did we miss connecting the dots?
9/11: A Brief Case Study of Missed Indications...
9/11: A Brief Case Study of Missed Indications...

- Between 1998-2001, at least 12 intelligence reports indicated Bin Laden planned to use aircraft and crash into buildings in NYC and Washington DC.

- Several indicators were present, however multiple agencies were not able to connect the dots to see a looming, imminent threat on the horizon.

- FBI admitted action could have been taken to harden cockpits and train pilots to resist hostile take over.

- May 18, 1998, FBI’s Chief pilot in Oklahoma City observed a “recent phenomenon” of Middle Eastern men taking flight training which “may be related to planned terrorist activity…” – his memo was not sent to FBI HQ.

- Subsequently, it was reported the hijackers in flight training were not interested in takeoff or landings, only wanted to quickly learn how to control a large aircraft after takeoff and sought to purchase advanced flight simulators.

- Intelligence started to reveal intentions of attack by aircraft, however analysts judged such an operation unlikely, because it did not offer opportunity of extremists to accomplish key goals.
**Byzantine Failure:** Lack of imagination coupled with inability to red team procedures and view how indicators could fit into a larger picture contributed to how warning signs were missed regarding this attack
We must be willing to evaluate our security stack using a Byzantine Failure Approach expecting a system to fail without notice or indication...

How do we still assure our critical information?
Attacks of Tomorrow from a Byzantine Perspective...

Which failures lead to compromise?
Attacks of Tomorrow from a Byzantine Perspective...

Which failures lead to compromise?
Attacks of Tomorrow from a Byzantine Perspective...

Attacks of Yesteryear started here…
Attacks of Tomorrow from a Byzantine Perspective...

Then evolved here…

- System Prog
- App Prog
- User Prog
- Library Routines
- System Calls
- Operating System
- Kernel
- Firmware
- HAL
- Hardware
Attacks of Tomorrow from a Byzantine Perspective...

Then evolved here…
Attacks of Tomorrow from a Byzantine Perspective...

What happens when the entire system is compromised?
And let’s never forget the User!

“Amateurs attack systems, Experts *attack* people…”
The impact cost of these attacks are huge!

Measured in the Billions per year! [BILLIONS]
Victory smiles upon those who anticipate the change in the character of war, not upon those who wait to adapt themselves after the changes occur.
Adjust your view of the World...

Were these Cyber Attacks?

Stuxnet
IoT: Could These Be Future Cyber Attack Platforms?

Home Security Systems
Amazon Echo, Google Home...
Smart Watches
Smart Devices
Smart TVs
Smart Homes
Could *These* Be Future Cyber Attack Platforms?

**Medical Devices:**
- Brain Neurostimulators
- Cochlear Implants
- Gastric Stimulators
- Cardiac Pacemakers
- Insulin Pumps
- EKG Monitoring

**Aviation Automation**

The Striking Similarities Between Lion Air and Ethiopian 737 MAX Crashes

**Transportation & Delivery Automation**
What does right look like?

Two roads diverged in a wood, and I — I took the one less traveled by

— Robert Frost
We cannot solve our problems with the same level of thinking we used when we created them.
What does right look like?

- New technologies (SDN)
- New security paradigms (e.g. Actionable-ThreatIntel, AI)
- New Secure Access Protection Systems
- New DLP Stack: data-at { rest, motion, transit}, platforms, and users
- Greater education (if defenders, developers, and attackers had the same knowledge... would exploits still exist?)
- Shift towards Prevention, Data isolation, Sandboxing, Segregation
- Non-attribution collaboration and information sharing (Best-practices)

What does YOUR recursive byzantine approach look like for:

- **ORGANIZATION**: Macro-analysis of data entering and leaving (which components are used to provide access data e.g. email, infrastructure, Internet, BYOD, WiFi/Bluetooth (and errant signals...), insiders, outsourcing, etc?) – trace how info can enter and leave the organization

- **SYSTEMS**: Micro-analysis of how components/devices/functions used to create/access/modify information (e.g. computer systems, devices, applications and programs, authentication protocols, integrity verification mechanisms, etc)
Tomorrow’s Victory is in Your Hands
My Charge to You!

- **I need you to be better;** Hackers are getting better, faster, smarter, more sophisticated… *why not you?*

- **I need you to be curious;** be bold; question the security paradigm; explore new options

- **Explore the possibilities** the unconventional attacker may introduce into your organization; *what did you previously dismiss as impossible?*

- **Recognize the indications** of the next cyber attack

- **Raise the cost** of the adversary just a little…

- **Change your approach:** Detection is too late → **Shift to prevention and resiliency**

- **Given an already compromised environment,** discover how we can still assure our tradecraft
What artifacts can we extract from a single domain?

www.domain.com

Name Server Information

nslookup

GEO Location

Registration Information

whois lookup

Domain Name
IPv4 server list
IPv6 server list
Domain Contact
Registrar
Domain Status
Servers
Registrant Contact
Name Servers
Update Date
Create Date
Tech Contact
Admin Contact
Zip
City
State
Country
Lat/Lon
IP
Domain

What artifacts can we extract from a single domain?
Excalibur Current Use Cases:

- Interface w/sensors applying IOCs for real-time identification
- Aggregate whois data from large domain name data sets
- Derive geo-location and nslookup info for each whois retrieval
- Uniform-structured data set from thousands of different registrars
- System Analysis sets correlating all artifacts based on identification
- Data enrichment via autonomous aggregation from DDS
- Connectors to addt’l Data Sources (VirusTotal, ThreatExpert, etc)
- Hunt for malicious indicators via Sim_Ref, XREF correlation
- Produce visualization graphs to derive meaning from data
- Convert large data sets of unknowns into most relevant IOCs

Maximize your utility by understanding Excalibur’s Use Cases
## Cyber Threat Detection System Components

- **Sensor - Packet Capture Library (actually intercept traffic)**
  - Wrapper/Packager (format, encrypt, transport data to analyzers)

- **Parser (analyzes sensory data)**
  - Profiles Network Traffic, Generate Alerts, Instigate Protection routines

- **Threat Intelligence Engine (Excalibur Mark I)**
  - Data enrichment: Feeds resolutions and IOC into the analyzer for real-time protection