

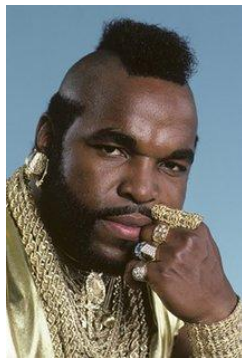
Something on Security

Guest Lecture - SE101, F'16

Mahesh V. Tripunitara

About me

- Associate Professor, ECE, tripunit@uwaterloo.ca
- Associate Director, SE, se-assoc@uwaterloo.ca
- Your “official” Academic Advisor, se-advisor@uwaterloo.ca
 - I sit in DC2597D, part of the SE suite of offices
 - You’re welcome to avail of Shaz Rahaman and/or Patrick Lam
- Students sometimes call me “Prof. T” or “Dr. T”
 - Not the same as this guy



Security Incidents

DDoS Attack Blamed for Massive Outages

Attack on DNS Company Dyn Suspected in Takedown of Twitter, Amazon and More

Matthew J. Schwartz [@mattjschwarz](#) · October 21, 2016 · 9 Comments

[Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#) [Email](#) [Print](#) [Get Notifications](#)

DDoS Attack Against Dyn Managed DNS
Incident Report for Dyn, Inc.

Resolved	The incident has been resolved. Posted about 13 hours ago (Oct 21, 2016 - 00:17 UTC)
Update	Our engineers continue to investigate and mitigate several attacks aimed against the Dyn Managed DNS infrastructure. Posted about 13 hours ago (Oct 21, 2016 - 00:09 UTC)
Update	Our engineers are continuing to investigate and mitigate several attacks aimed against the Dyn Managed DNS infrastructure. Posted about 13 hours ago (Oct 21, 2016 - 00:07 UTC)
Update	At this time, the advanced service monitoring issue has been resolved. Our engineers are still investigating and mitigating the attack on our infrastructure. Posted about 13 hours ago (Oct 21, 2016 - 00:02 UTC)
Update	Dyn Managed DNS advanced service monitoring is currently experiencing issues. Customers may notice increased error rates in their advanced DNS records. Our engineers continue to monitor and investigate the issue. Customers with questions or concerns are encouraged to reach out to our Technical Support Team. Posted about 13 hours ago (Oct 21, 2016 - 00:00 UTC)
Update	Our engineers continue to investigate and mitigate several attacks aimed against the Dyn Managed DNS.

(This story has been updated.)

Online Ad Industry Threatened by Security Issues

Voluntary Set of Anti-Malware Guidelines May Not Go Far Enough

Jeremy Kelle [@jeremy_kelle](#) · October 21, 2016 · 0 Comments

[Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#) [Email](#) [Print](#) [Get Notifications](#)

MALVERTISING

The online advertising industry is at an inflection point, and not just from falling ad rates, ad blockers and potential regulation. It's facing a big security problem, and one that - like many internet-scale problems - will demand close industry cooperation to be mitigated.

Russian Indicted for Breach of Three Silicon Valley Companies

Suspect Said to Have Targeted LinkedIn, Dropbox and Formspring

Eric Chabrow [@erichabrow](#) · October 22, 2016 · 9 Comments

[Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#) [Email](#) [Print](#) [Get Notifications](#)

LinkedIn

A U.S. federal grand jury in Oakland, Calif. indicted a 29-year-old Russian man for hacking computers at three Silicon Valley companies - social networking sites LinkedIn and Formspring and file-sharing company Dropbox.

3.2 Million Indian Debit Cards at Risk

Banks Alerted Up to Six Weeks Ago; Investigations Ongoing

Narain Harash [@NarainHarash](#) · October 21, 2016 · 0 Comments

[Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#) [Email](#) [Print](#) [Get Notifications](#)

The National Payments Council of India confirmed Oct. 20 that more than 3.2 million debit cards issued by Indian banks may have been compromised.

NSA Contractor's Alleged Theft 'Breathtaking'

Judge Orders Harold T. Martin III To Be Jailed Until Trial

Jeremy Kelle [@jeremy_kelle](#) · October 21, 2016 · 2 Comments

[Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#) [Email](#) [Print](#) [Get Notifications](#)

NATIONAL SECURITY AGENCY

Harold T. Martin III, a Black Albanian American contractor, worked with the NSA

(This story has been updated.)

Video on Alleged Medical Device Flaws Stirs Controversy

Tactics of Investment Firm, Researchers in Attacking St. Jude Medical Questioned


Benjamin Kibuka McGee [@BenjaminKibuka](#) · October 20, 2016 · 0 Comments

[Twitter](#) [Facebook](#) [LinkedIn](#) [Reddit](#) [Email](#) [Print](#) [Get Notifications](#)

ST. JUDE MEDICAL

Story has been updated to include FDA response.









Let's pick one...



DDoS Attack Blamed for Massive Outages

Attack on DNS Company Dyn Suspected in Takedown of Twitter, Amazon and More

Matthew J. Schwartz (@euroinfosec) · October 21, 2016 · 0 Comments



DDoS Attack Against Dyn Managed DNS Incident Report for Dyn, Inc.

Resolved	This incident has been resolved. Posted about 12 hours ago. Oct 21, 2016 - 22:17 UTC
Update	Our engineers continue to investigate and mitigate several attacks aimed against the Dyn Managed DNS infrastructure. Posted about 12 hours ago. Oct 21, 2016 - 22:00 UTC
Update	Our engineers are continuing to investigate and mitigate several attacks aimed against the Dyn Managed DNS infrastructure. Posted about 12 hours ago. Oct 21, 2016 - 21:30 UTC
Update	At this time, the advanced service monitoring issue has been resolved. Our engineers are still investigating and mitigating the attacks on our infrastructure. Posted about 16 hours ago. Oct 21, 2016 - 18:52 UTC
Update	Dyn Managed DNS advanced service monitoring is currently experiencing issues. Customers may notice incorrect probe alerts on their advanced DNS services. Our engineers continue to monitor and investigate the issue. Customers with questions or concerns are encouraged to reach out to our Technical Support Team. Posted about 16 hours ago. Oct 21, 2016 - 18:23 UTC
Update	Our engineers continue to investigate and mitigate several attacks aimed against the Dyn Managed DNS

(This story has been updated.)

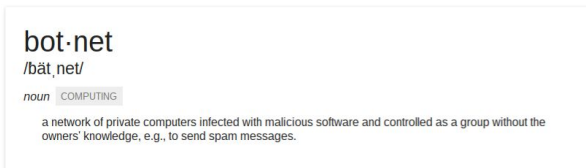
What we observed

- Popular websites “down”
 - Amazon, Twitter “unreachable”

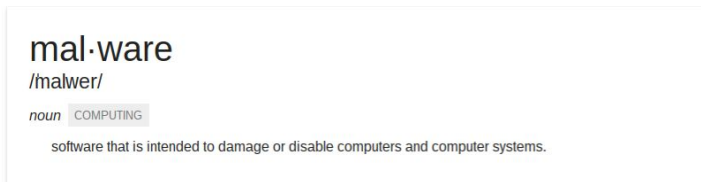
So, security property that was violated: *Availability*.

Under the covers, (1)

- DDoS = “Distributed Denial-of-Service”
- Not directly against those sites, but against an infrastructure component
 - The “Domain Name System,” DNS
- A botnet bombarded a DNS provider with junk packets



- Malware with which each member of the botnet was infected: Mirai.



Under the covers, (2)

Ah, so a root-cause was allowing the Malware to be installed and run...

How did that happen?

- Attackers logged in and installed them
 - Remotely
 - On millions of devices
-
- How? What kind of devices?

Under the covers, (3)

- Device allowed logging in remotely
 - E.g., ssh program
- Devices had superuser accounts with default passwords
 - Passwords well-known - in user's manual

So, security property that was violated: *Authenticity*.

Authenticity, (1)

au·then·tic·i·ty

/ˌɒtHentɪsədē/

noun

the quality of being authentic.

"the paper should have established the authenticity of the documents before publishing them"

synonyms: genuineness, [bona fides](#); [More](#)

au·then·tic

/ɒtHen(t)ɪk/

adjective

1. of undisputed origin; genuine.

"the letter is now accepted as an authentic document"

synonyms: [genuine](#), [real](#), [bona fide](#), [true](#), [veritable](#); [More](#)

2. **MUSIC**

(of a church mode) comprising the notes lying between the principal note or final and the note an octave higher.

Authenticity, (2)

- Entity that installed malware is not “real” superuser as claimed
 - That is, that entity is not “authentic.”
- Two different kinds of authenticity:
 - an identity
 - of data



Under the covers, (4)

- Ok, so the authenticity property was violated
- Anything else?
- Somewhat perversely, availability worked against us.
 - (Rationale on next slide.)

Under the covers, (5)

Investigation of the attack uncovered 49,657 unique IPs which hosted Mirai-infected devices. As previously reported, these were mostly CCTV cameras—a popular choice of DDoS botnet herders. Other victimized devices included DVRs and routers.

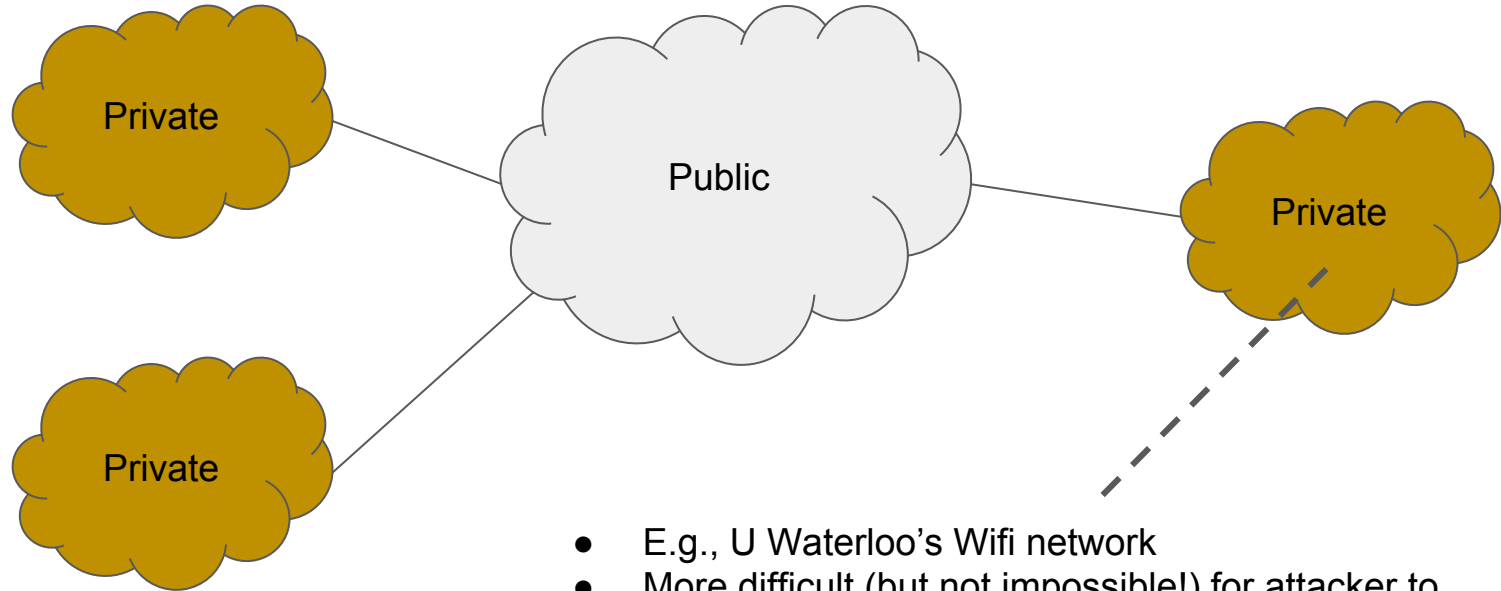
Mirai's "Don't Mess With" List

One of the most interesting things revealed by the code was a hardcoded list of IPs Mirai bots are programmed to avoid when performing their IP scans.

This list, which you can find below, includes the US Postal Service, the Department of Defense, the Internet Assigned Numbers Authority (IANA) and IP ranges belonging to Hewlett-Packard and General Electric.

```
127.0.0.0/8      - Loopback
0.0.0.0/8        - Invalid address space
3.0.0.0/8        - General Electric (GE)
15.0.0.0/7       - Hewlett-Packard (HP)
56.0.0.0/8       - US Postal Service
10.0.0.0/8       - Internal network
192.168.0.0/16   - Internal network
172.16.0.0/14    - Internal network
100.64.0.0/10    - IANA NAT reserved
169.254.0.0/16   - IANA NAT reserved
198.18.0.0/15    - IANA Special use
224.*.*.*+      - Multicast
6.0.0.0/7        - Department of Defense
11.0.0.0/8       - Department of Defense
21.0.0.0/8       - Department of Defense
22.0.0.0/8       - Department of Defense
26.0.0.0/8       - Department of Defense
28.0.0.0/7       - Department of Defense
30.0.0.0/8       - Department of Defense
```

The Internet, roughly

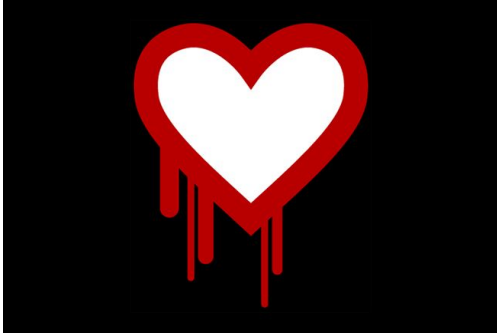


- E.g., U Waterloo's Wifi network
- More difficult (but not impossible!) for attacker to initiate session.

Under the covers, (6)

- So: a bunch of little devices (e.g., CCTV cameras)
 - Were on the publicly-routed Internet (available - to the attacker)
 - With poor password-protection (poor authentication)
-
- A low-brow attack
 - Are more sophisticated attacks possible?
 - Yes!
 - More significant security properties can be violated, e.g., privacy, integrity, ...

Example, (1)

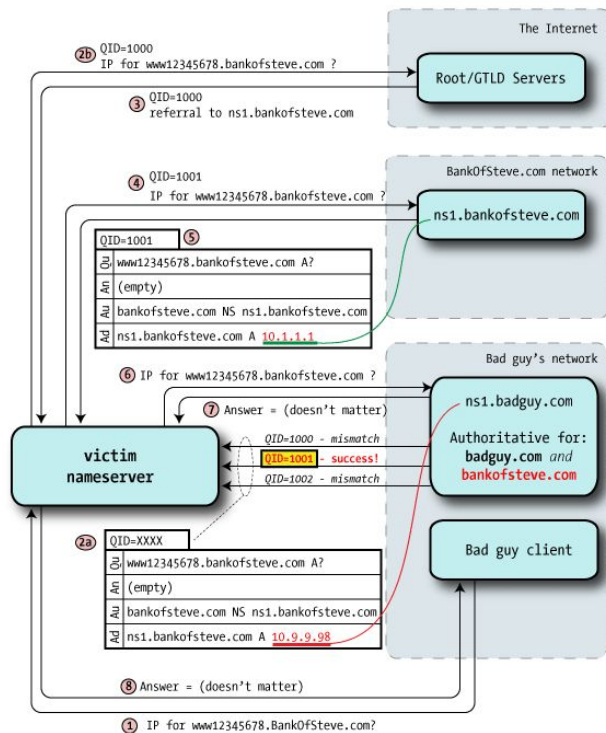


- See <https://xkcd.com/1354/>

Example, (2)

- DNS: used to map names to numbers
 - E.g., mailservices.uwaterloo.ca → 129.97.128.141
- Kaminsky attack on DNS
 - See <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>
 - “An Illustrated Guide to the Kaminsky DNS Vulnerability”

Example, (2) (contd.)



fin

tripunit@uwaterloo.ca