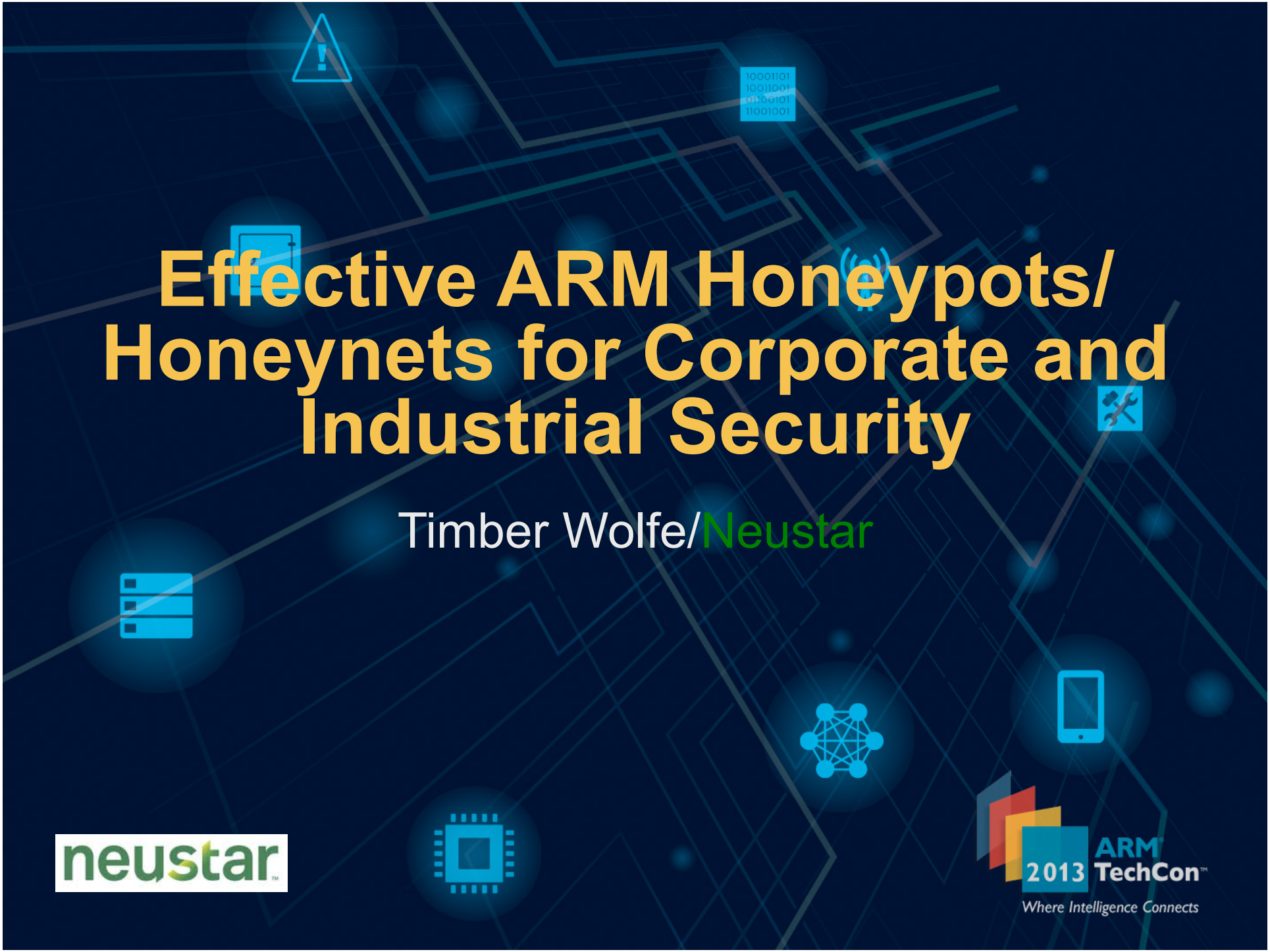

ARM®
2013 TechCon™
Where Intelligence Connects
UBM
Tech



Effective ARM Honeypots/ Honeynets for Corporate and Industrial Security

Timber Wolfe/Neustar

neustar

ARM 2013 TechCon
Where Intelligence Connects

Honeypot Introduction

Why an ESC?

- Uses Atheros devices and conceptually works with any embedded system, yielding out of the box solutions
- Can be utilized to protect your embedded networks, which are typically vulnerable

Suggested Skillsets

- Programming/Scripting
  - C, C++
  - **Python**
  - Assembly (Intel) and IDA
  - Experience with Debuggers and Disassemblers
- Windows System Internals
- Linux System Internals
- Threat Analysis Skills
- Computer Forensics Knowledge

Note: www.safaribooksonline.com

Concepts and Usage

Concepts and usage of a wireless honeypot

Psychology of usage?

- Attacking your wireless
  - They must be close or have gear close
  - They bypass all of your IDS/IPS/DLP/Central network logging gear
- Why use this?
  - The attackers MAC address can be obtained and used in black lists for adjacent and remote networks.
  - These attacks can be targeted (hacktivism). An attacker can be attacking multiple facilities. Building a MAC black list of people attacking networks adjacent to yours will be useful. This is a preventative measure.
- Psychology
  - Hackers consider this a 'free' target of opportunity. As such, they will rarely build defenses when wireless networks are first attacked.
  - They can hit it from afar with little to no chance of detection nor have fear of actually being caught. This honeypot does not negate this yet.
  - Consider the ESSID of the honeypot. It should be enticing.
  - Consider the PW used for the wireless connection.
    - Do not make it too difficult or too simplistic.
    - Do not use words like 'yourtrapped', etc. The attacker will see this before connecting to the network. This kind of thing could scare them off and **you want that MAC address**.

Protect the Integrity of the Honeypot

- Infection Detection
  - Momentary wireless connections are allowed (provides an opportunity for exploitation)
  - Could be exploited from the inside of the network (LAN side)
  - Detection: Take an Whirlpool hash of the firmware prior to deployment, as well as any other relevant files (PW file).
  - Detection: Use a HAF (Honeypot Application Firewall) for monitoring the traffic traversing the router and the device running the python scripts. The HAF would have a few rules/RE's hunting irregular traffic.
  - Did the ESSID change?
  - Did the ESSID PW change to one not in the file?
- It must be given a little attention now and again.
  - Log rotation not implemented
  - Monitoring hashes (of firmware, python, pw file, etc…)
  - Low maintenance as connections will only be numerous while testing.

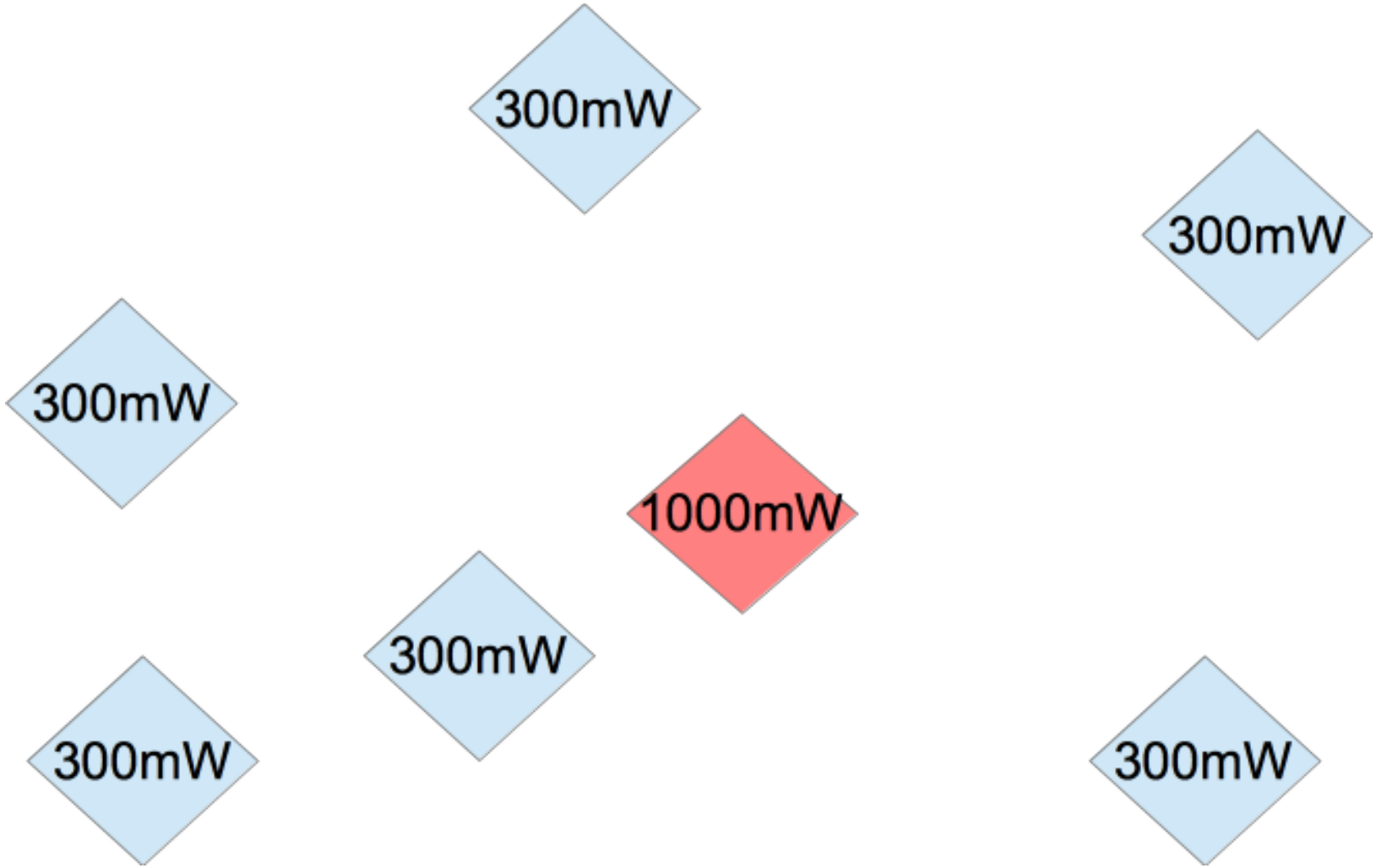
Parallels

- This ideology can be directly applied to other technologies
  - Blue Tooth
  - ZigBee
  - Aduino
  - Pineapple of Death
  - 802.11 devices
- For effectiveness:
  - Monitor the LAN for devices (Banner Grabbing)
  - Monitor ARP for MAC address list not in whitelist. Should be notified of any changes to MAC addresses on monitored networks. (rogue access points, cell phones, embedded recording devices)
- Consider custom sniffers
- Consider HOP counts and latency. This can be automated. (Heuristic Checks)

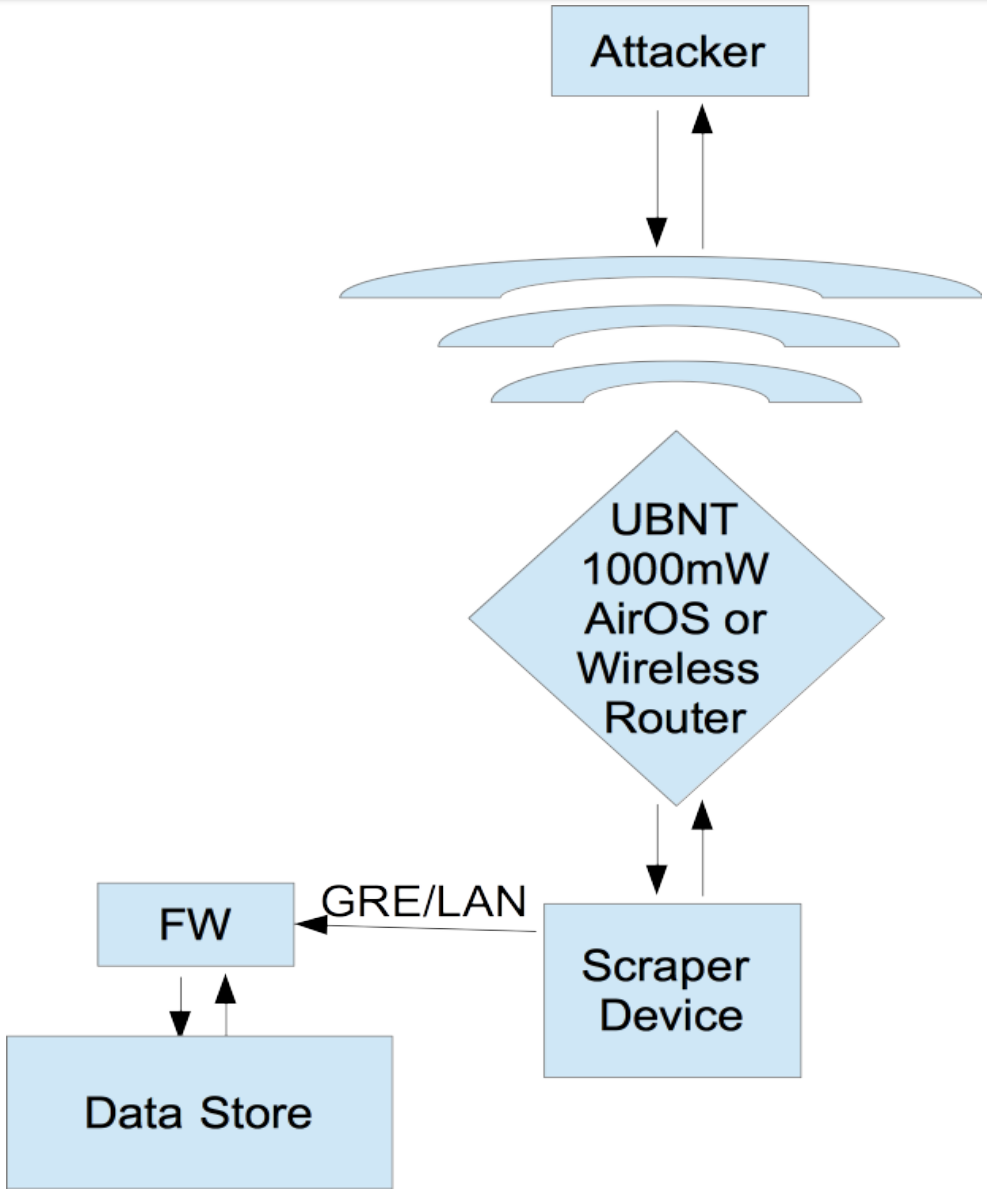
General Security

- Paste bins should be monitored for corporate name, IP's, specific marketed items that do not have common names
  - www.scapy.org contains a framework for this, put what you want to look for in a database.
  - There are LAN and AP databases all over the net (Google used to have one)
  - Look for open source tools related to this soon
- Do not wear branded clothing to security conferences
- LAN security techniques should be vastly different than WAN security.
  - LAN's and control networks wont change without your knowledge (not true of the WAN).
  - LAN's and control networks are relatively fixed in size compared to that of a WAN
  - Do not forget to think outside of the box!

Wireless Honeypot Mesh Deployment



Wireless Honeypot Deployment



Netgear WG602Vx Specifics

- Approximate transmit power: 100-500 mW
- Inexpensive
- Negative Factors over High Power Device:
  - Large physical footprint
  - Requires Power Cord (no POE on consumer models)
  - Power uniform in a mesh configuration

*Note: these stats would apply to just about any desktop grade networking gear as would the UBNT specifications to most commercial or carrier grade gear.

UBNT Device Specifics

- Upside:
  - Transmit Power: up to 1000mW TX power at 8W
  - Inexpensive (~$130.00)
  - POE (one cable)
  - Very small physical footprint
  - Weatherproof design / UV protected / Carrier Grade Gear
  - 8W consumption in normal run mode
  - Will stand out in a crowd (ie: in a mesh network this will be a huge target)
  - TX power adjustable on the fly
- Many configuration possibilities with different antennas
- AirOS is used on a wide range of their devices (**so one honeypot can be used w/out modification on an array of products**).
- These sensors are very powerful and if used in a mesh over a wide area/ campus can pinpoint a crackers location. Live gear on this network would have to possess a client capable of pulling rogue MAC addresses from the database that have been collected.
- AirOS is extensible
- http://www.ubnt.com/airos
- http://www.ubnt.com/airrouter

For Pentesters

- UBNT could be deployed in a PVC pipe in the ground or on/inside of a vehicle (uses POE)
- Question for the audience:
  - Is there interest in a pineapple load?

SHODAN for the LAN

- SHODAN is a fancy banner grabber.
- I may include a banner grabber to accompany this presentation.
- Consider logging the initial scan and periodic ones in between to note trends and metrics related to particulars
- This banner grabber will log what it finds on the network
  - Consider the ports that should be scanned
  - Some devices may be overlooked if the correct ports are not scanned
  - To properly generate a banner, the port may require some input other than just the connection

Honeypot Usage on the LAN for APT Detection

- How do you search out APT's on the LAN now?
- How else could you?
- A honeypot on the LAN would detect the scanning activity of an APT trying to propagate as well as malfunctioning hardware

What's Next?

- Open WRT romanHunter functionality
- Possible UBNT native functionality
- Pen Testing Tools
- Modern Honeynet in a box

Implementation of romanHunterv3

How to obtain, install, configure
and run romanHunterv3. A demo will be included

romanHunterv3c Components

- Requires a device capable of running python scripts
  - These scripts will scrape and update the router in response to scraped data
- Wireless router, a Netgear WG602x
  - Will soon work with a UBNT AirOS device (www.ubnt.com) ← Atheros chipset (this technology is independent of the hardware used, hence the flexibility)
- How it works:
  - The scraper will monitor the page that displays the MAC addresses on the router that are associated and authorized.
  - If an authorized one is found, the scripts will write the MAC address out to the log file; then read the last pw used out of the log file, open the pw file, select the next one on the list. If no matches are found between the last one used in the log file and the pw file, the first one on the list will be used by default. The associated MAC addresses are only logged for use in metrics over time.
  - The scripts change the pw on the router
  - The process repeats

What's missing 1?

- Log scraper (capture the logs remotely)
- Email alerting
- Automating process of black listing MAC addresses, found on the honeypot, on adjacent and other corporate networks. (not performed by this software)
- Perform some work with the associations. They are only displayed on the screen and or captured in the log. This could provide very valuable metrics. For example, if the same MAC appears over and over again over a short period of time – it could represent someone trying to brute force the attack. This particular honeypot is not capable of capturing the pw's being attempted.
- Culling of the log file (lots of work to do here) and formatting of the output.
- Monitoring for a crash
- Implement error checking/correction/notification

What's missing 2?

- **romanHunterV3c Add-Ons**:
  - Functionality for central repository usage for all to share
    - Real-time list additions (as MAC's are discovered add them to the central database repo)
    - Periodic additions for closed network usage (Industrial Networks)
    - Information repo for how this collection facility was used and what type of LAN it was used on (Industrial/Corporate)
    - Small Questionnaire, nothing specific, 100% voluntary, those whom volunteer their data will have free access to the data.
  - MAC whitelist functionality

Conclusion

- **Remember the pineapple Jasager app?**
  - **When your wireless powers up it says "are you my connection x"?**
  - **This could now be used against the attacker as the connection to the honeypot 'has been made'. If they are lazy, which most wireless hackers are totally brazen and fearless, they will not scrub their connections lists.**
  - **This could be used at all coffee shops, areas of dense population (like a city) for tracking where the hackers live, are congregating, where they are meeting regularly, where they are hacking regularly, etc…**
  - **Could be used for non-repudiation**
- **Keep in mind that one single scraper could monitor hundreds of wireless devices over a large network.**
  - Key differences would be:
    - It would have to monitor which device it logged the information from
    - It would have to be efficient if it was scaled up
    - Would need a way to 'disable' the wireless in the event the scraper were losing power or malfunctioning. ie: Make it robust

Demonstration Time!

- Who wants to be an attacker?

Banner Grabbing
(SHODAN)

Banner Grabbing Code Demonstration
and why its important to perform on a LAN

Why is Banner Grabbing Important

- This can be implemented on the scripting device used for the wireless router scraper
- This can be implemented on a tiny, inexpensive device (useable for penetration testing), so it can be used on segmented networks as well
- The psychology here is not to find something to use but to find devices that should not be here, to facilitate that we need a central device list repo.
- Can be used for vulnerability scanning

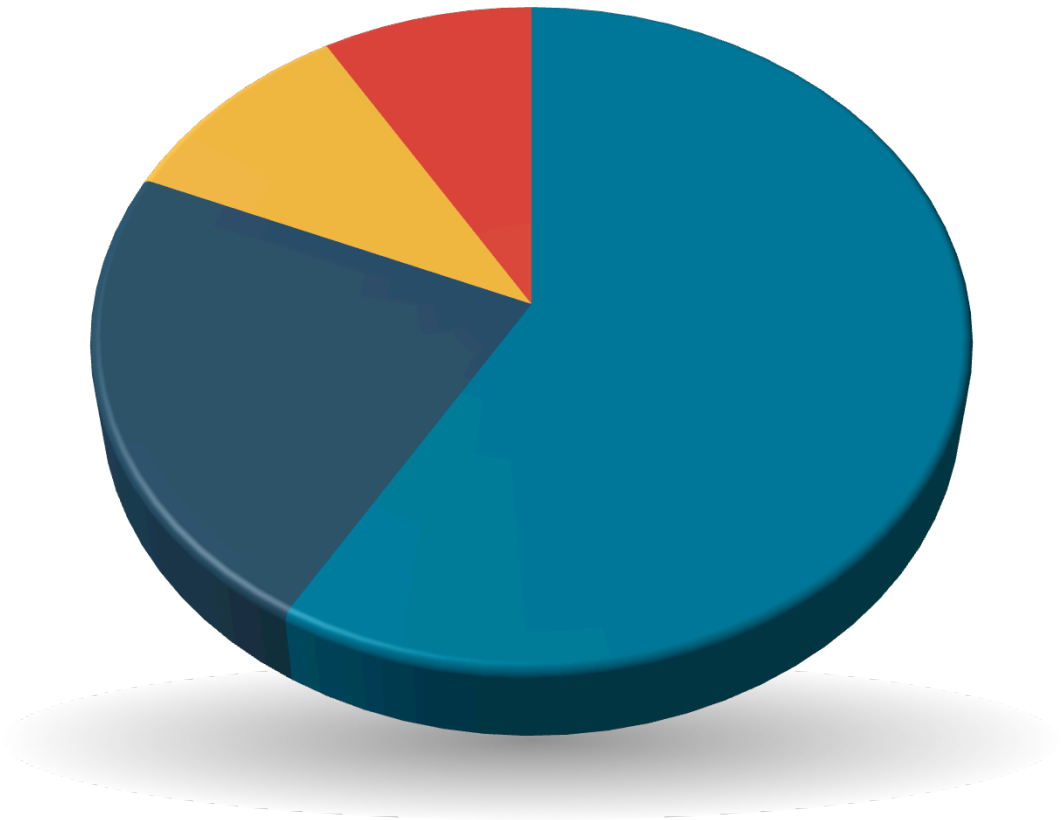

Timber Wolfe
Effective ARM Honeypots/Honeynets for Corporate and Industrial Security
lonegray@gmail.com
neustar
2013 ARM TechCon
Where Intelligence Connects


ARM®
2013 TechCon™
Where Intelligence Connects
UBM
Tech

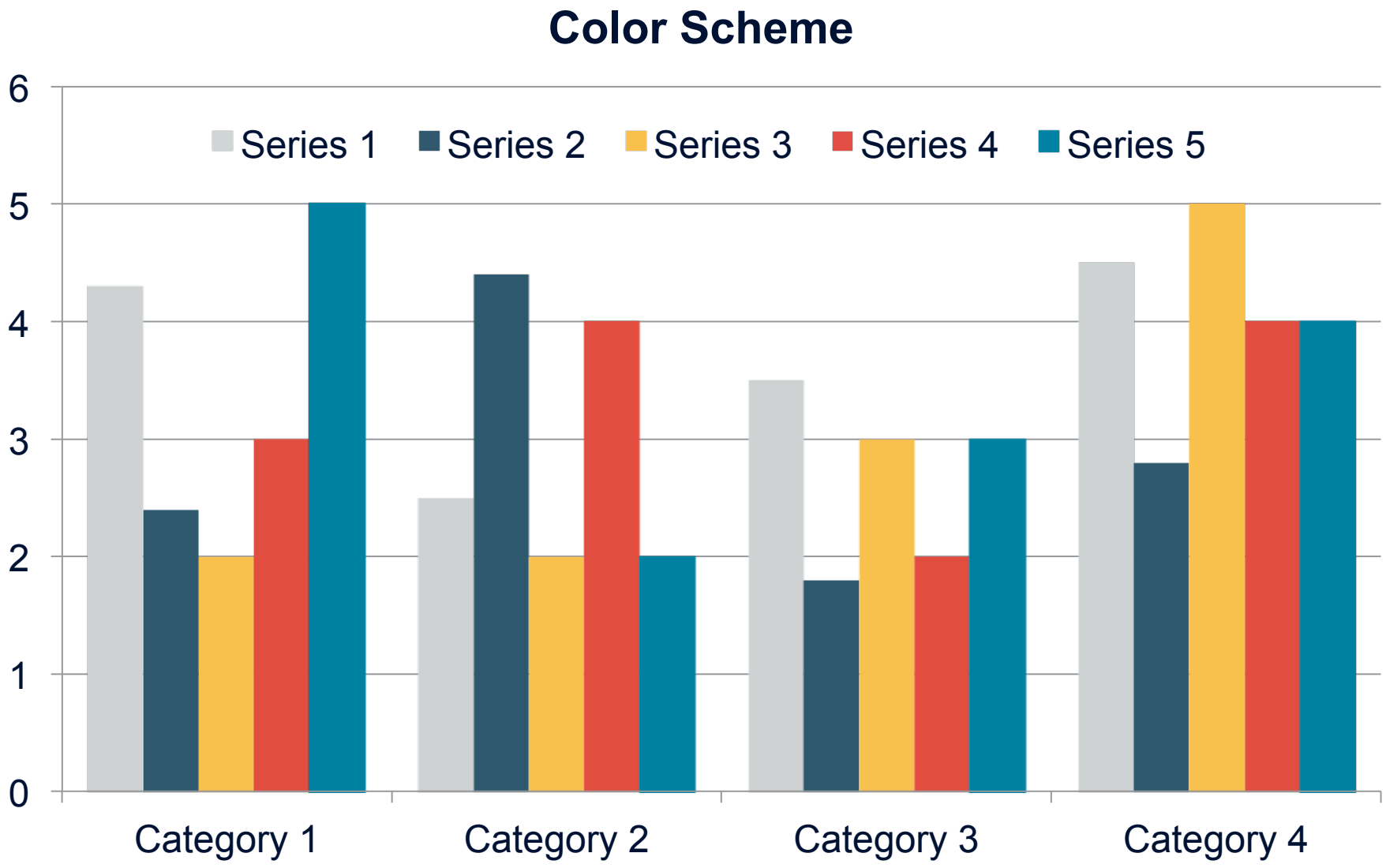
Section Header

Divider

Pie Chart



Bar Chart


Color Scheme
6
5
4
3
2
1
0
Series 1
Series 2
Series 3
Series 4
Series 5
Category 1
Category 2
Category 3
Category 4