RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CXO-R02

What Sennacherib Taught Me About Security: How to Translate Cyber-speak

Mary Ann Davidson
CSO
Oracle Corporation
@heenaluwahine

Program Agenda

1. Cybersecurity and … Cuneiform?
2. A History Lesson: Sennacherib
3. Storytelling Resources
4. Deep Dive: Military History
5. Conclusion

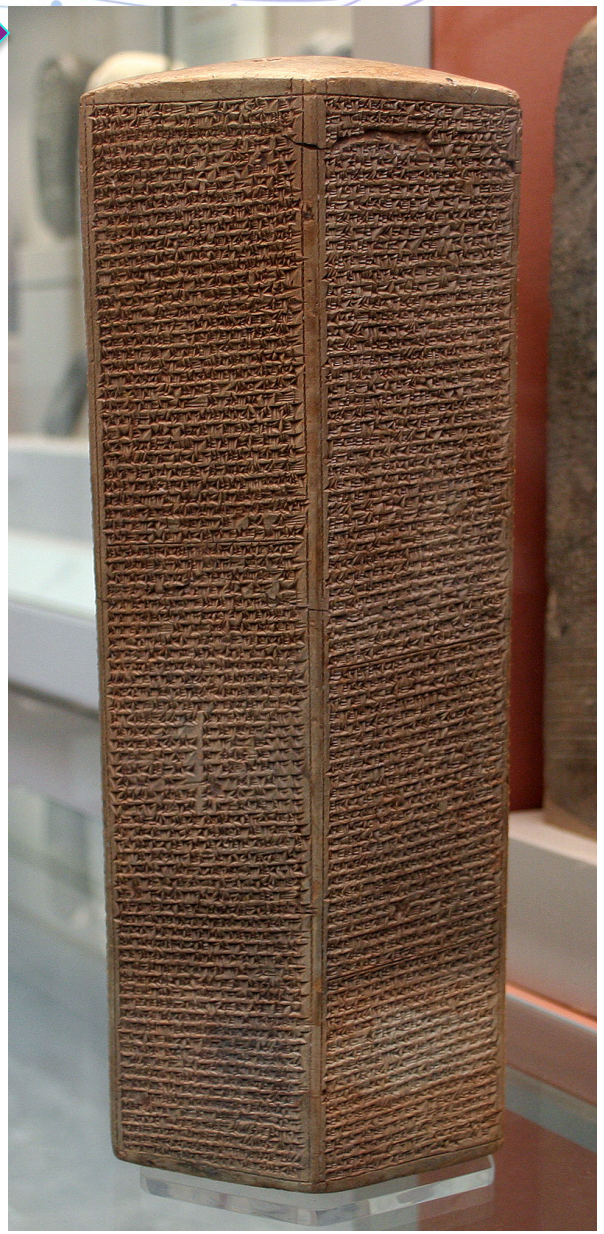
Cybersecurity and Cuneiform, Seriously?

- Both…
  - Begin with ‘C’
  - Are incomprehensible to many
  - Require “translation services” for non-experts to understand
  - …including Why It Matters
- And…
  - Cybersecurity is too important to be left to experts
  - “Translation” may also cause *us* to think and talk about security differently
    - …leading to “Eureka!” moments

Sennacherib: A Brief Bio

- Son of Sargon II
- King of Assyria 705–681 BCE
- Rebuilt the city of Nineveh and made it his capital
- (Possibly) creator of the famous Hanging Gardens of Babylon
- Known for military campaigns against Babylon and Judah
- Died in 681 BCE (killed by his son(s))

Sennacherib: Facebook and Blog



Translate, Please…

א וַיְהִי בְּאַרְבַּע עֶשְׂרֵה שָׁנָה לַמֶּלֶךְ חִזְקִיָּהוּ, עָלָה סַנְחֵרִיב מֶלֶךְ-אַשּׁוּר עַל כָּל-עָרֵי יְהוּדָה הַבְּצֻרוֹת--וַיִּתְפְּשֵׂם.

I ka makahiki umikumamaha o ke alii, o Hezekia, pii ku e mai la Sanekariba ke alii o Asuria, i na kulanakauhale a pau i paa i ka pa o ka Iuda, a hoopio iho la ia lakou.

(Now it came to pass in the fourteenth year of king Hezekiah, that Sennacherib king of Assyria came up against all the fortified cities of Judah, and took them. (Isaiah 36:1))

A History Lesson: Sennacherib's Siege of Jerusalem

- Described in the Bible (Isaiah, 2 Kings, 2 Chronicles)
- Well-attested outside the Bible
  - Siege of Lachish (British Museum reliefs from Sennacherib's palace at Nineveh)
  - Described on three cuneiform prisms (Taylor, Oriental Institute, Jerusalem)
  - Archeological evidence (e.g., Siloam Tunnel to Gihon Spring, Jerusalem)
- Why It Matters

See, It Really Happened (1)

Assyrian Siege Ramp – Lachish

See, It Really Happened (2)

Inscription: “Sennacherib, the mighty king, king of the country of Assyria, sitting on the throne of judgment, before (or at the entrance of) the city of Lachish (Lakhisha). I give permission for its slaughter…"

Takeaways

- Stories and analogies have meaning for people
- Stories can illustrate lasting truths, even about ephemeral topics (like much of technology)
- Stories can help translate complexity into ideas people “get”
- Stories can reinforce desired cultural norms
- All of which are **really** important when we are talking about cybersecurity…

Storytelling Resources (1 of 2)

- Your *own* experiences
  - …including “corporate history”
  - …and not just “security stories!”
- Literature
  - “There is nothing new under the sun…”
- Economics/Finance
  - Because resources are always limited…

Storytelling Resources (2 of 2)

- Humor
  - "A merry heart doeth good like medicine"
- Biology
  - Trees defend themselves better than we do…
- Military history
  - "He who defends everything defends nothing."

Some Caveats Before We Begin

- Technical knowledge *is* important
  - "You gotta know the territory!"
  - "Double XOR – twice as strong as XOR!"
  - Using analogies helps *you* understand what you just learned about the geeky bits
- Examples herein I've used successfully
  - Abject failures are conveniently omitted…

My Own Experiences…

- “You can’t add rebar after the concrete has set…”
- “Closed, not a bug…”
- “Why would anybody do that?”
- LDAP and obsession
- “This is bad…”
- “Our own IT department wouldn’t accept this risk…”

Weapons in The Explanatory Arsenal

- Literature
  - How Joshua DOSed Jericho
  - The Little Dutch Boy
- Economics
  - Crowding out effect
  - Opportunity cost
- Humor
  - Sugar bombs
- Biology
  - The Dangers of Monoculture
- Military History
  - The Battle for Guadalcanal

Pulling It All Together…

- The military has a lot to teach us about cultural ethos, defensibility and “the battlefield”
- …which can transform the way we think about, talk about and change cybersecurity…

Changing the Battlefield:
Innate Defensibility of Software

- **What we build** can and will change the network battlefield
- "Every Marine a rifleman…"
  - Marines are a lethal fighting force with a strong warrior ethos
  - Marines "assume an enemy" and prepare for war
  - …including the next war
- Implications
  - Each developer must be personally responsible for the security of his/her code
  - Products must self defend, every one of them
  - Mentality shift in development to disallowing every other possible future use instead of allowing all possible future uses

Changing the Battlefield:
Self-Awareness of the Network (1)

- Lack of situational awareness is caused by lack of basic information
  - Who's on my network?
  - What is on my network?
  - *What is my "mission readiness" (performance, bandwidth, security posture)*
- Causes
  - You can't correlate non-existing data
  - Some standards for threat information exchange
  - Value add is the BI component, not "translation services"

Changing the Battlefield:
Self-Awareness of the Network (2)

- Government could enforce such standards as a public good
  - Example: Transcontinental Railroad
  - Or find other ways (procurement, “certifications”) to force the market to provide situational awareness
- Could enable “dynamic redoubts”
  - Lessons from the defense of Rorke’s Drift
  - Reconfiguring networks and products that go to “DEFCON-n” when under attack
  - …because attacks are automated, defenses may need to be automated, also

Changing the Battlefield:
Innate Defensibility of Data

- "He who defends everything defends nothing." - Frederick the Great
- Search (and-destroy) engines?
  - The corollary to information lifecycle management is what you should *not* have/use/keep
  - GDPR may provide an incentive for automated data destruction
    - Might also be a market differentiator
- More flexible access models?
  - Self sealing/time-to-live data (SnapChat-ish)
  - Narrow risk/attack vector through more contextual access (time of day/pattern of use/who do I think you are/what device are you using)

Changing the Battlefield:
E-M Theory Applied to Networks

- Fighter pilots “win” based on agility (Boyd’s energy-maneuverability (E-M) theory)
- OODA (observe, orient, decide, act)
  - OODA was an air warfare concept that changed the face of war (notably in Gulf War I)
  - And has been applied to other disciplines
  - Is there applicability to cyber-offense and defense?

Conclusions

- "There is nothing new under the sun"
- Use stories to tell a story!
- Security is *not* just about technology, but also:
  - …helping people understand fundamental principles, concerns and remedies
  - …reinforcing security as a cultural norm
  - **…and knowing the limits of technology**


Q&A