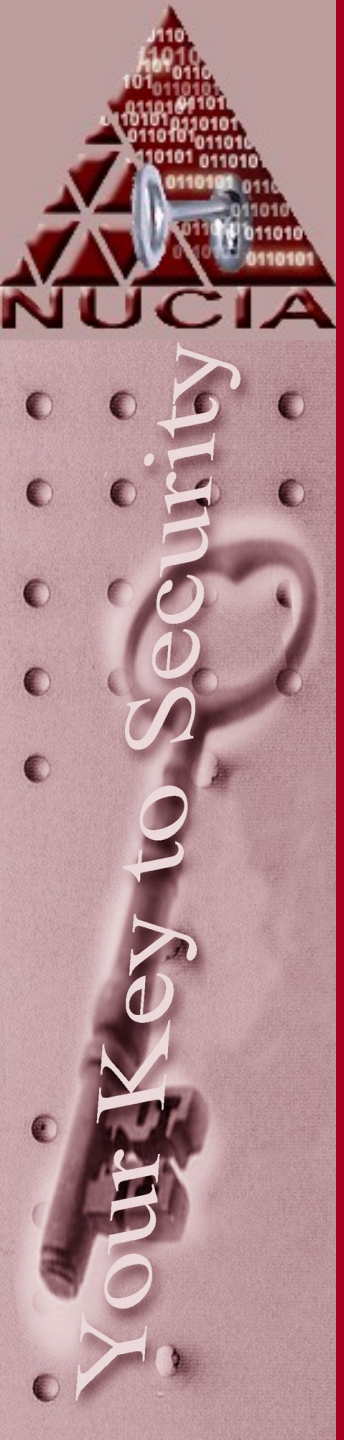


Nebraska University Consortium on Information Assurance

NE-Cert KEYNOTE

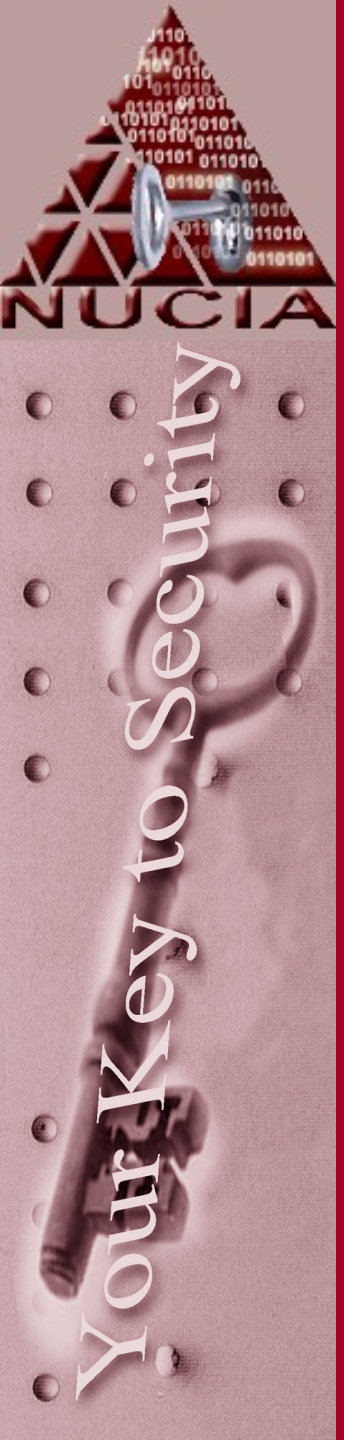
Blaine W. Burnham, PhD
Executive Director,
Nebraska University Consortium for Information Assurance,(NUCIA)
College of IS&T
Peter Kiewit Institute
University of Nebraska, Omaha

NE Cert

- Outline
  - Changing nature of the Threat
  - The Robustness of the Technology
  - The Rising Sophistication of the Attacks
  - An Opportunity?

NE Cert

- Changing nature of the threat
  - Definition
    - Threat: agent, means, motive, opportunity
      - Agent: The bad guy or his surrogate
      - Means: Included the vulnerabilities
      - Motive: The Return – Why
      - Opportunity: Access(ready or contrived

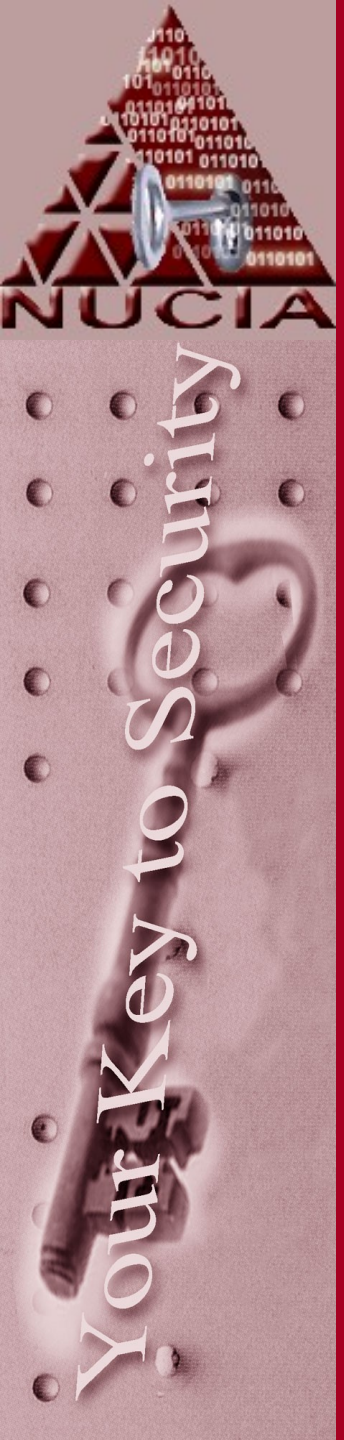


NE Cert

- Changing nature of the Threat
  - Historical
    - Three “layers” of the Threat
    - Low end, the cyberspace Vandal
      - In it for the Noise
      - Tended to be visible to highly visible
    - High End, The Nation State
      - In it for information / long term
      - Tended to be very not visible
    - The Middle, The Cyber Mercenary
      - In it for the Money and the things Money can buy
      - Depends on the approach

NE Cert

- Changing nature of the threat
  - Going after the money!!
    - Evolving to a industry
      - Well organized
      - Very well funded
      - Service oriented
        - » Customized produces
  - The vandal is all but gone.
    - Clever “vandals” are finding offers “ too good to refuse” and being swept up into the industry.

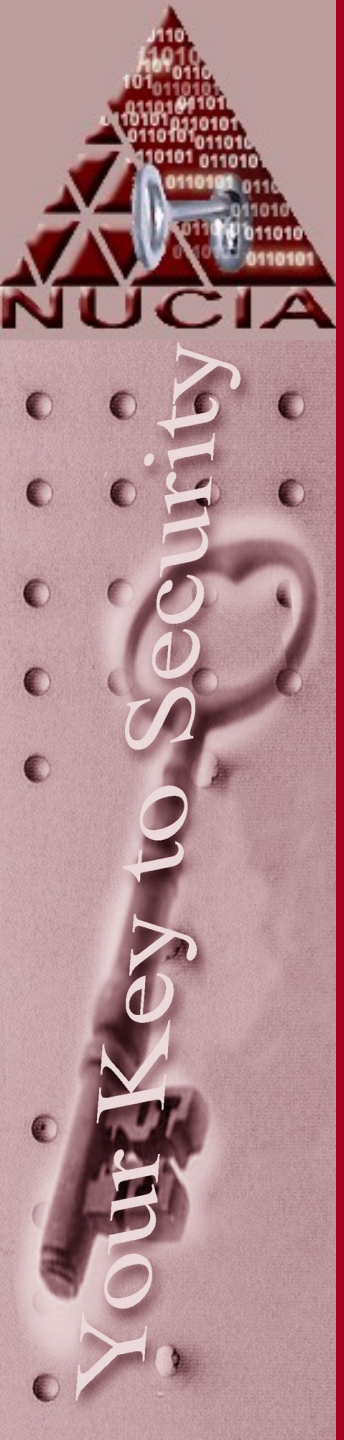


NE Cert

- The Robustness of the Technology
  - Hardware hacking is on the rise
  - About RFID
    - Market claim: RFID numbers are unique
    - Implementations assume uniqueness of RFID numbers
    - Demonstrated Cloning of RFID numbers / devices
    - Worse: The Near Field Communications feature in emerging mobile phones
      - The phone – with appropriate software – ca act as an RFID tag, an RFID reader, a pseudo server to one client and a pseudo client to another server
      - An awesome man-in-the-middle attack engine
      - Business models that rely on RFID for low-value payments will find there systems spoofed
      - Consider the RFID based subway payment model – the electronic purse. The appropriately configured NFC phone – will loot the e-purses just walking by.
  - Push is on wrt Bluetooth
    - Each one of those little ear devices would make a great listening device.

NE Cert

- The Rising Sophistication of the Attacks
  - The Web Worm
    - Hybrid Worm, runs on both the client and server side
    - Starts in and infected machine, infects the Browser, then uses the credentials of the infected Browser to advance the attack to Server and then back to the Clients.
    - Considerable shared code since it is running in application space. The attack code is fairly lite
    - Has a polymorphic code modifier
    - Signature based search tools will be less and less useful.



NE Cert

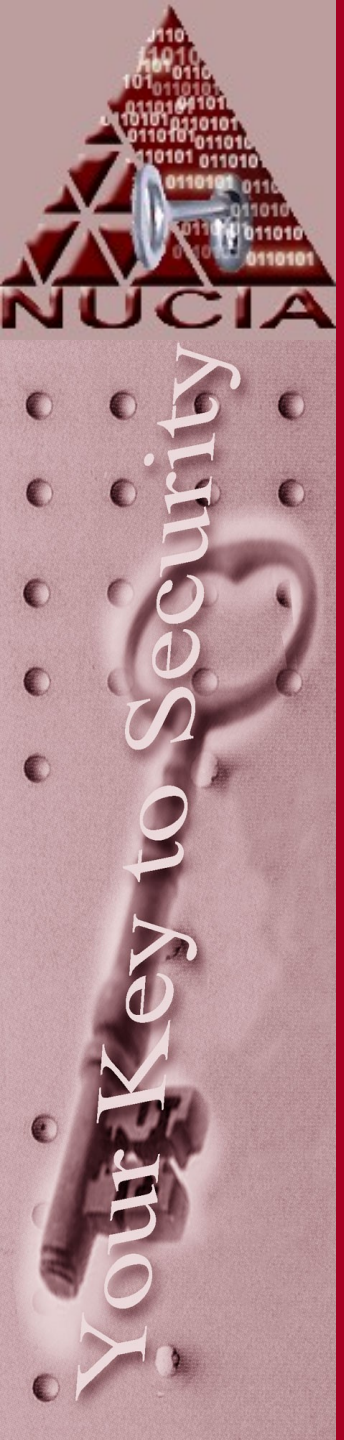
- An Opportunity?
- Unforgivable Vulnerabilities
  - Steve Christy / Mitre
  - A discussion of Vulnerabilities that just shouldn't happen any more
    - Technique for selection
    - Both of:
      - Many have made the same mistake
      - The mistake is well documented
    - Two of
      - The attacks are obvious
      - The manipulations are simple
      - Able to be found with 5 minutes effort

NE Cert

- An Opportunity?
- Unforgivable Vulnerabilities
  - They Are:
    - Jump to Whitepaper
- Reasonable Question
  - Why are we still making these mistakes
    - Can't we do anything.
  - How about making the awareness of these mistakes part of the hiring process.
  - We expect proficiencies in languages, why not expect our new hires to be aware of these mistakes and demonstrate the ability to find them in and not make them.
  - Put the pressure on the schools to teach this stuff in the mainstream CS programs as part of software engineering.

NE Cert

- Summary
  - The bad guy is getting very much badder.
  - The motives are Money
  - The attacks are changing
    - Growing Sophistication and Stealth
    - The home computer is a prime target
      - The botnet providers love the home user
      - There is no substantial help for the home user
      - Telecommuting off the home computer could not be a worse idea
  - Maybe, just maybe we can encourage a small difference by requiring security awareness in our workforce.



NE Cert

- Ramblings
  - Web Enabled services are problematic
    - If you cannot make some very strong arguments re the extent of the service domain you are likely hosed.
  - Missing Identity records / stolen identities
  - E-voting