USB Forensics and Pentesting

Dr. Phil Polstra

PhD, CISSP, CEH

@ppolstra

http://philpolstra.com

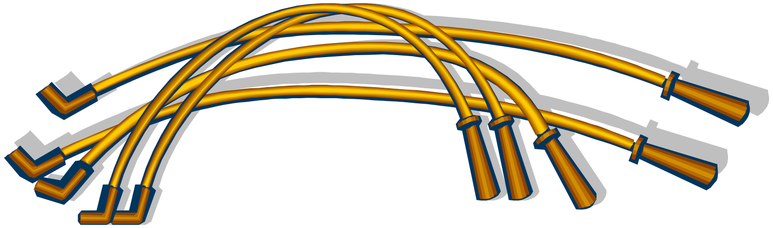
Certifications:
http://www.securitytube-training.com

Pentester Academy:
http://www.PentesterAcademy.com

USB Basics: Endpoints

Endpoints

- The virtual wire for USB communications
- All endpoints are one way (direction relative to host)
- Packet fragmentation, handshaking, etc. done by hardware (usually)
- High bit of address tells direction 1=in 0=out
- Types of endpoints
  - Control
  - Bulk transport
  - Interrupt
  - Isochronous



Control Endpoints

- Primary mechanism for most devices to communicate with host
- Every device must have at least one in and out control endpoint EP0
- Device must respond to standard requests
- Get/set address, descriptors, power, and status
- Device may respond to class specific requests
- Device may respond to vendor specific requests

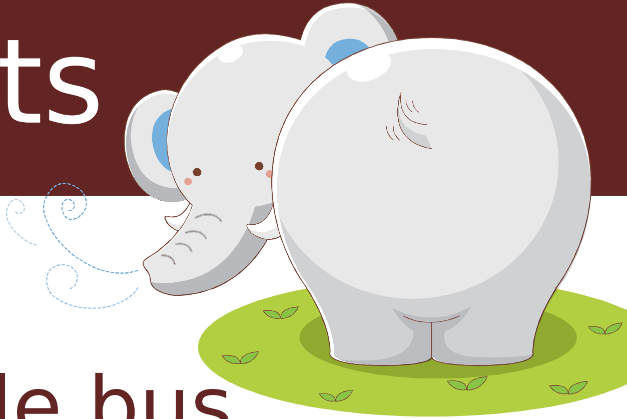
Control Endpoints (cont.)

- May have up to 3 transport stages: Setup, Data, Status
- Setup stage
  - Host sends Setup token then data packet containing setup request
  - If device receives a valid setup packet, an ACK is returned
  - Setup request is 8 bytes
  - 1st byte is bitmap telling type of request & recipient (device, interface, endpoint)
  - Remaining bytes are parameters for request and response
- Data stage (optional) – requested info transmitted
- Status stage – zero length data packet sent as ACK on success

Interrupts & Isochronous Endpoints

- Interrupt endpoints
  - Used to avoid polling and busy waits
  - Keyboards are a good example
  - Usually low speed (allows for longer cables, etc.)
- Isochronous endpoints
  - Guaranteed bandwidth
  - Used primarily for time-critical apps such as streaming media

Bulk Endpoints



- No latency guarantees
- Good performance on an idle bus
- Superseded by all other transport types
- Full (8-64 byte packets) & high speed (512 byte packets) only
- Used extensively in USB flash drives (and external hard drives)
- Transactions consist of a token packet, 0 or more data packets, and an ACK handshake packet (if successful)

Endpoint Demo