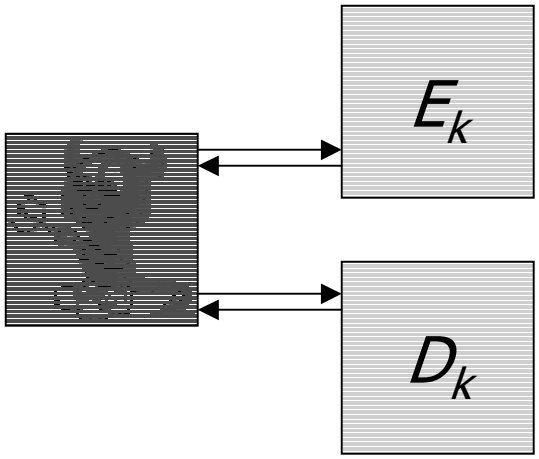
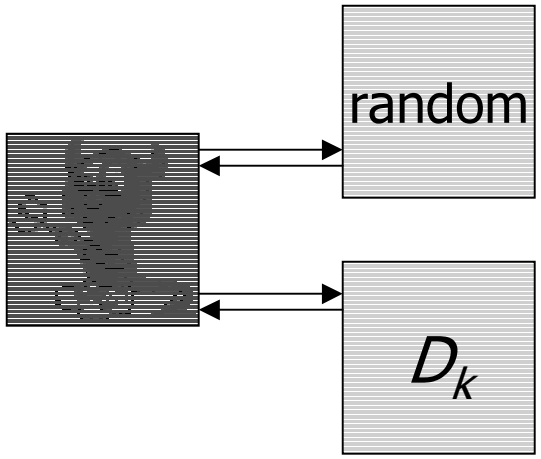
# Crypto Theory and Security Practice

David Wagner
*University of California at Berkeley*

# Theory: IND-CCA2, INT-CTXT




Universe 1

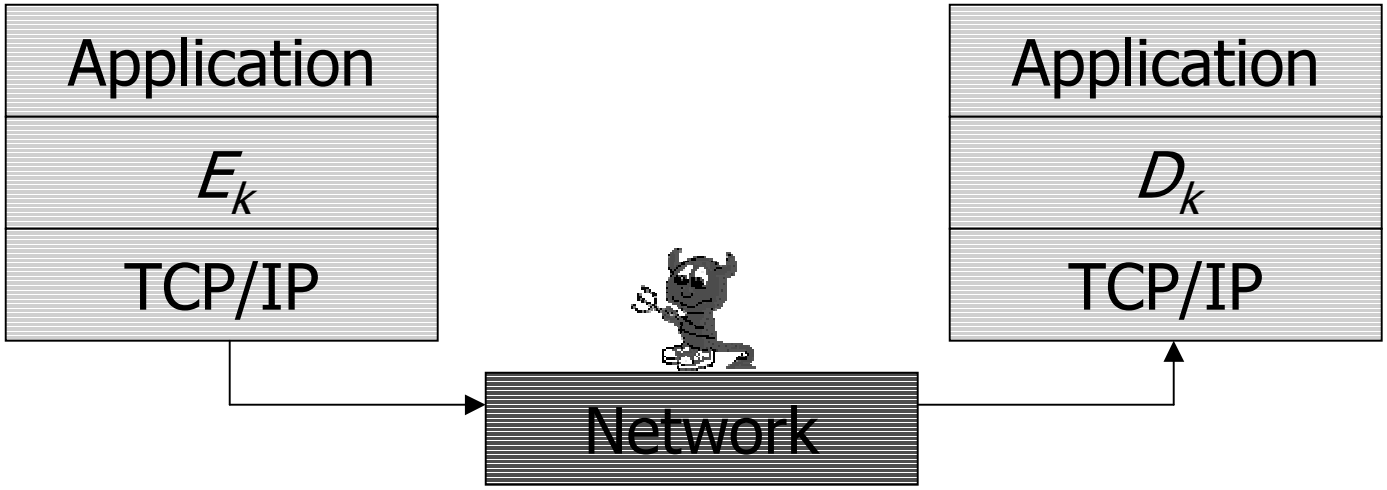



Universe 2

IND-CCA2 = no attacker can distinguish between universes $\Rightarrow$ Confidentiality

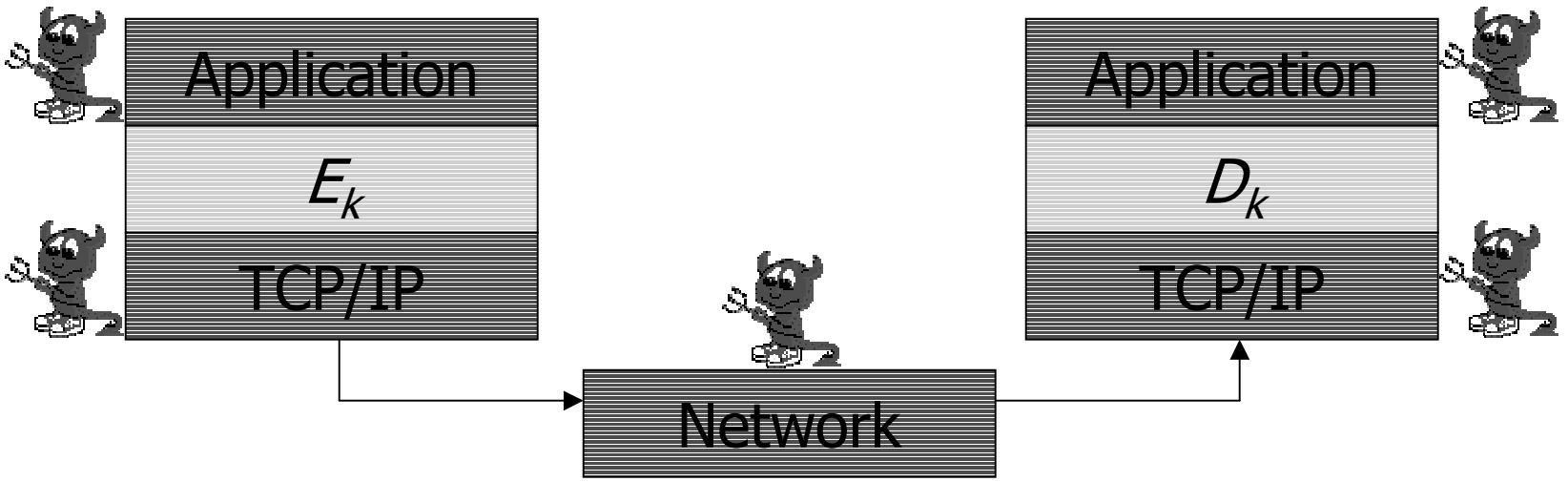
INT-CTXT = no attacker can forge a new ctext $\Rightarrow$ Integrity

# Practice: Layering Principles




Design principle: Crypto layer should not make any assumptions about other layers

# Practice: Layering Principles

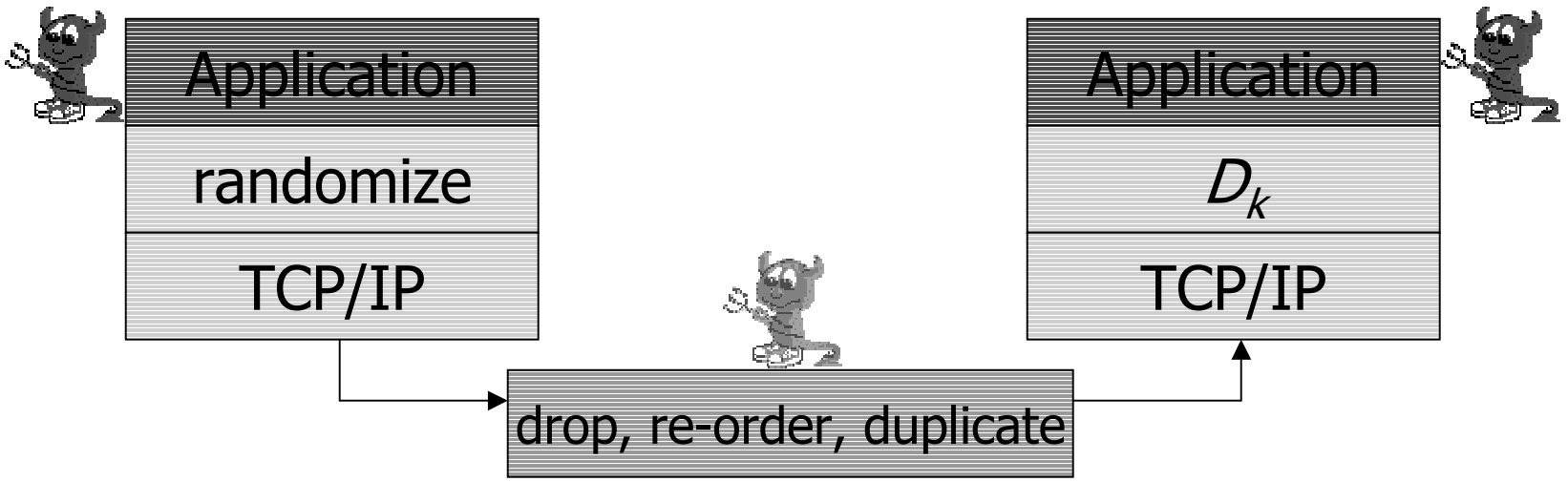



Design principle: Crypto layer should not make any assumptions about other layers, i.e., crypto should ensure security *even if all other layers are malicious*

Interesting, this is just what IND-CCA2, INT-CTXT guarantee

# More Precisely…

Anything you can do with chosen-plaintext/ciphertext, you can do with less:



# Summary

- Crypto theory is highly relevant to engineering practice
- Composition is where the action is
- Wanted: a theory of security for systems, not just crypto primitives