Malformed Bytes

Tom Roeder and Christian Paquin
Microsoft Research

I’m thinking that it’s fine
when a message from the client
comes so many times
and when the padding comes out misaligned

And I have to speculate
that the Docs themselves
did make us into oracles
that have a plaintext puzzle pieces rate

And true, you may not like to MAC
but it’s code like this
that catches XOR’d messages
and turns the adversary’s errors back

When you are out there in the wild
with several thousand megabytes
of phony messages
I hope this song will guide you right

They will send us packets of malformed bytes

“Respond now”, they’ll say

But errors leak our secrets from far away

“Respond now”, but we’ll wait

I tried my best to leave
this all on your PC
but the resistant code review team
was short on listening

And that frankly will not fly
you will hear the shrillest cries
and loudest moans with CBC mode
when the hackers 0wn your code

They will send us packets of malformed bytes

“Respond now”, they’ll say

But errors leak our secrets from far away

“Respond now”, but we’ll wait

Original Song: Such Great Heights

by the Postal Service

Arrangement: Iron and Wine

Parody Lyrics: Tom Roeder

Guitar: Christian Paquin